Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Model of the information security protection subsystem operation and method of optimization of its composition

Basil Al-Kasasbeh

Faculty of Computer Studies, Arab Open University, Saudi Arabia

ARTICLE INFO

Article history:
Received 21 December 2021
Revised 15 April 2022
Accepted 22 May 2022
Available online 2 June 2022

Keywords:
Information security protection subsystem
Artificial threats to information security
Protective mechanisms
Optimization
Confidentiality

ABSTRACT

Increasing threats to the confidentiality and integrity of information require careful consideration of the problem of its protection. This is confirmed by the constantly spreading information about successful hacker attacks. Thus, the problem of securing information that has financial, competitive, military or political value is extremely relevant. However, increasing confidentiality should not forget about its antipode – availability. An effective information security protection subsystem must ensure a rational balance between the values of these dependability attributes. Analytically, this concept of balance can be embodied in the task of optimizing the values of the characteristic parameters of such a subsystem. At the same time, the concept of efficiency should be extended to such a mathematical apparatus. Its complexity should ensure the adequacy of the description of the information protection process but not be excessive to ensure that it can be applied. Based on these initial provisions, the article presents a method of operational optimization of the composition of the information security protection subsystem, taking into account the aggressiveness of cyberspace in which the target information system is operated. The method is formalized in the paradigm of Markov chains with the approach to the formulation of the classical optimization task, which is classified as nonlinear discrete. Considering the lack of a universal method for solving such mathematical programming tasks, the article adopts the method of sequential variants analysis for such purposes. The results of the experiments proved the adequacy and functionality of the proposed method.

1. Introduction

We live in an era of total digital transformation. We may be just at the beginning of this process, but experience has shown that we are accustomed to the convenience of high technology, but underestimate the potential threats to information security. Dependence on technology creates many risks for people, businesses and countries. No one is insured against these risks, and even the largest and most respected corporations can face financial, reputational or even human losses at any time. Cyberattacks have ceased to be a narrow IT problem and have become a real threat to society and business. Thus, the issue of information security protection is currently hyper-relevant.

2. State-of-the-art

One of the most important tasks in the field of information security is a qualitative threat assessment. It is the reliable result of such an assessment that is the basis for a rational choice of means and methods of information protection. There are several well-known tools for assessing information security, modelling of security measures, and possible types of threats to information security, the main of which are presented in [1–5]. In particular, we mention probability theory and mathematical statistics, fuzzy sets, game theory, graph theory, the theory of digital automata, Petri nets, the theory of random processes, and so on.

These methodologies form a toolkit for analyzing the performance of the studied information systems for a finite censored period of time. The analysis takes place in the context of determining: 1. The time period between failures in the studied system; 2. The num-

E-mail address: bkasasbah@arabou.edu.sa

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2022.05.003

ber of failures in the studied system for the censored period of its operation; 3. The reaction of the studied system to the provoked failures; 4. The reaction of the studied system to complex test effects.

Models [6–9] were created with a focus on the description of the first performance indicator. They are based on the mathematical apparatus of time series analysis. Their purpose is to identify the parameters of the statistical distribution, which best describes the period between failures in the operation of the studied system. The adequacy of such models is determined by the representativeness of the sample of data that characterizes the operation of the studied system. When formalizing such models, only the fact of failure is taken into account without analyzing the causes of its occurrence and possible consequences.

Models [10–13] were created with a focus on the description of the second performance indicator. It is assumed that the stochastic parameter, which characterizes the number of time failures, is described by a certain distribution law (most often Poisson's) with a continuous or discrete intensity function. The latter is determined by the results of static analysis of operational data. The disadvantages of this type of model are similar to those mentioned above.

Models [14–17] were created with a focus on the description of the third performance indicator. The data for analysis in these models are: – the number of failures in the studied system for the censored period, which were caused by unknown negative impacts; – the number of failures in the operation of the studied system during the censored period, which were caused by negative impacts, the mechanisms of counteraction of which were embedded in the studied system at the stage of its design. Data analysis is carried out by combinatorics and maximum likelihood methods. Such models are more informative, but are still based on information, some of which was collected as a result of uncontrolled experiments.

Models [18–22] were created with a focus on the description of the fourth performance indicator based solely on the results of controlled experiments. Considering that the causes of failures are usually interrelated, models of this type are based on the mathematical apparatus of Markov chains. This allows us to take into account the multithreading in the operation of the studied system and the heterogeneity of the process of its recovery after failure. The behavior of real information systems is more accurately described by semi-Markov models, because the process of recovery of the first ones after failures can be characterized not only by the exponential distribution functions. The structural features of the studied system in this approach to modeling can be taken into account in the graph of the flow of control, which brings the model closer to the described process. This qualitatively distinguishes the Markov approach from, for example, nonparametric neural network [23–25], in which the structure features of the studied system are ignored.

Considering the above, we will focus on the Markov approach to the description of the process of operation of the studied system in the conditions of aggressive cyberspace. Close analogues are the models of information systems confidentiality based on discrete Markov chains described in articles [18–22]. These models are based on elements of reliability theory and describe the studied information system as a system with failures and recoveries. In the mentioned studies, the process of operation of the studied system is formalized in the metrics of absolute qualitative indicators of the theory of reliability, while the economic aspect is completely ignored. However, the results presented by the authors of these studies have shown that Markov processes can be used to model negative impacts on information systems if the first ones can be considered stochastic and independent. Based on these postulates, the use of Markov processes to model the operation of information systems is permissible.

The ***object*** of the study is the process of counteracting the information security protection subsystem (ISPS) impact of artificial threats to information security (ATIS). The ***subject*** of the study is the theory of Markov random processes for the analytical description of the object and the theory of mathematical programming for the statement and solution of the corresponding optimization task. The ***aim*** of the study is the analytical formalization of the optimal scheme of information security (SIS) in the target information system.

3. Materials and methods

3.1. Statement of research

Suppose that the software ISPS (formed by a conglomerate of software protective mechanisms) of some information system with probability q_i is affected by ATIS of i-type, . Accordingly, at any time the studied information system can be: – in functional state 0 if the actual impact of any ATIS is not or ISPS has successfully neutralized the impact of the corresponding ATIS (the probability of this event is characterized by the parameter R_i); – in a state of counteraction to the i-th ATIS if the corresponding negative impact is realized and ISPS counteracts it; – in the non-functional state $n+1$ if the ISPS has not been able to neutralize the effect of the corresponding ATIS (the probability of this event is characterized by the parameter $1-R_i$). The process of operation of the information system described in this way is presented in Fig. 1 by the UML state diagram.

Analytically, such a stochastic process can be described by a Markov chain with the following matrix of probabilities of transitions between states:

$$\Pi = \begin{pmatrix} 1-\sum_{i=1}^{n} q_i & q_1 & q_2 & \dots & q_n & 0 \\ 1-R_1 & 0 & 0 & \dots & 0 & R_1 \\ 1-R_2 & 0 & 0 & \dots & 0 & R_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \qquad (1)$$

Thus, the ***objectives*** of the study are 1. Analytically formalize in the paradigm of Markov chains the relationship between the set of ATIS and the structured ISPS in the appropriate quality metric; 2. Based on the received mathematical apparatus to carry out a statement of the optimization task for the composition of ISPS taking into account that the target information system at the set moment has to be in a functional condition with the corresponding probability; 3. To test the proposed method of operational optimization of the composition of ISPS for a real information system and analyze the results.

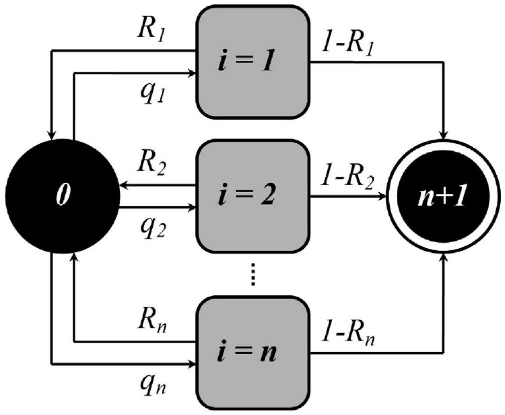

Fig. 1. UML state diagram of the studied process.

3.2. Mathematical model of the studied process

Suppose that at the initial moment of censored observation the information system is in functional state 0. The probability of the information system in state $j \in J = \left\{\overline{0, n+1}\right\}$ at a discrete-time $t = 1, 2, \ldots$ is determined based on the matrix (1) and the state in which the system was at the time $t - 1$:

$$p_j(t) = \sum_{i=0}^{n+1} p_i(t-1)\Pi_{ij} \tag{2}$$

Using expression (2) we present, taking into account the matrix (1), the probability of the studied system in the appropriate state as a function of time:

$$p_0(t) = \frac{(q_0 + w)^{t+1}}{w2^{t+1}} - \frac{(q_0 - w)^{t+1}}{w2^{t+1}} \tag{3}$$

$$p_j(t) = q_i p_0(t-1) i \in I \tag{4}$$

$$p_{n+1}(t) = 1 - p_0(t) - p_0(t-1)\sum_{i=1}^{n} q_i \tag{5}$$

where $q_0 = 1 - \sum_{i=1}^{n} q_i$ and the parameter

$$w = \sqrt{q_0^2 + 4\sum_{i=1}^{n} q_i R_i} \tag{6}$$

is a generalized characteristic of the effectiveness of ISPS.

If the censored time interval is large enough, then the second term in expression (3) goes to zero. Considering this fact, we obtain a simplified version of expression (3):

$$p_0(t) \approx \frac{(q_0 + w)^{t+1}}{w2^{t+1}} \tag{7}$$

Despite its simplicity, the model generalized to expressions (3)–(5) is sufficiently functional to quickly assess the vulnerability of ISPS configured with parameter (6) to counteract the set of typed ATIS. Due to the stochastic nature is visualized in Fig. 1 model of the process of operation of the studied information system, at some time moment the system will transit into a non-functional state $n + 1$. We formalize analytically the dependence of the duration of the studied information system in a functional state 0, despite the probable influence of ATISs, taking into account the composition and settings of the ISPS.

In terms of classical reliability theory, the parameter that characterizes the average censored time before the transition of the system from a functional state to a non-functional one is the mean time between failures (MTBF). Considering that the created mathematical apparatus is focused on operational application, as well as the fact that the studied information system has a structured ISPS, instead of the MTBF parameter we will use the parameter τ, which determines the time at which the probability of being characterized by the matrix (1) information system will be halved relative to the value of this probability at the time $t = 0$:

$$p_0(\tau) = \frac{1}{2} p_0(0)$$

Express the desired parameter τ from expression (7):

$$\tau = \log_{\frac{1}{2}(w+q_0)}\left(\frac{1}{2}w\right) - 1$$

Let us evaluate analytically the conditions under which the value of the characteristic parameter τ will exceed the value of the censored time interval $[0, t_0]$:

$$t_0 \leqslant \tau = \log_{\frac{1}{2}(w+q_0)}\left(\frac{1}{2}w\right) - 1 \tag{8}$$

Present in inequality (8), the parameter q_0 characterizes the generalized probability of the influence of an arbitrary ATIS from the set I on the studied information system. We need to determine the range of allowable values of the parameter $w = f(R_i)$, $i = \overline{1, n}$, at which inequality (8) holds.

Convert inequality (8) to the form

$$\frac{1}{2}w \leqslant \left(\frac{1}{2}(q_0 + w)\right)^{t_0+1} \tag{9}$$

Inequality (9) characterizes the constraints for protective mechanisms in the structure of ISPS, expressed as a set of parameters $R = \{R_i\}$, $i = \overline{1, n}$. We formalize the process of solving inequality (9) concerning the parameter w. After the implementation of typical transformations we obtain:

$$w \geqslant 2R^* - q_0 \tag{10}$$

where $R^* \in [q_0, 1]$ is the real root of the equation

$$R^{t_0+1} - R + \frac{1}{2}q_0 = 0$$

To calculate the constraints on the values of the characteristic parameters, we substitute expression (10) into expression (6). As a result, we obtain the following inequality:

$$\sum_{i=1}^{n} q_i r_i \geqslant R^*(R^* - q_0) \tag{11}$$

The obtained inequality (11) together with the restrictions on the values of the characteristic parameters R: $0 \leqslant R_i \leqslant 1$, $i = \overline{1, n}$, determine the boundaries of the convex domain of the allowable values of the characteristic parameters of the protective mechanisms in the structure of ISPS in the parametric space $R_{t_0}\left(\{q_i\}, i = \overline{1, n}\right) \subset R_+^n$. Based on the preconditions embodied in the expression (11), we can say that only for the values of the characteristic parameters, which belong to the domain $R_{t_0}\left(\{q_i\}, i = \overline{1, n}\right)$, inequality (8) holds.

After determining the domain of allowable values $R_{t_0}\left(\{q_i\}, i = \overline{1, n}\right)$ for which the inequality $\tau \geqslant t_0$ is satisfied, it is logical to take the next step and analytically describe the process of finding the optimal values of the characteristic parameters $R^* \in R_{t_0}\left(\{q_i\}, i = \overline{1, n}\right)$ for protective mechanisms in the structure of ISPS of the studied information system. Let us correspond to each j-th, $j = \{\overline{1, m}\} = J$, protective mechanism in the structure of ISPS a set of binary values x_i, $i = \overline{1, n}$, of the form

$$X_j = \left(\{x_i\}, i = \overline{1, n}\right) \in \{0, 1\}^m \tag{12}$$

where the parameter $x_i \in X_j$ is 0 if the j-th protective mechanism is involved in counteracting the i-th ATIS, or the parameter $x_i \in X_j$ is 1 if the j-th protective mechanism is not involved in counteracting the i-th ATIS.

We introduce the parameter $R_{i,j}$, $i \in I, j \in J$, which corresponds to the probability that the j-th protective mechanism neutralizes the effect of the i-th ATIS. A complete set of m vectors of the form (12) integrally characterizes the ability of a structured ISPS to counteract a certain multiplication of n ATISs. Moreover, considering the content of the sets of the form (12), to counteract the i-th ATIS can simultaneously several protective mechanisms. This fact can be analytically described by the expression

$$R_i(X) = \sum_{\gamma=1}^{m} (-1)^{\gamma-1} \sum_{j_1<j_2<\ldots<j_\gamma} \left(R_{i,j_1} x_{j_1}\right) \times \\ \times \left(R_{i,j_2} x_{j_2}\right) \times \ldots \times \left(R_{i,j_\gamma} x_{j_\gamma}\right). \tag{13}$$

In expression (13) the classical dilemma "confrontation of a sword and a shield" is put. On the one hand, the higher the probabilities $R_i(X)$, the more efficient the ISPS will be. On the other hand, the amount of system computing resources is always limited, so the loss of ISPS, which is manifested in the fact that the i-th ATIS is aimed at more than one protective mechanism, leads to reduced information security of the studied information system as a whole because confidentiality and availability become competing attributes. The natural way out of the revealed paradox is to set the optimization task for the process of functioning of the studied information system generalized by the matrix (1).

We introduce the parameter c_j which will characterize the resource consumption of the j-th protective mechanism in the structure of ISPS, $j \in J$. Accordingly, the event of the activation of the configuration of protective mechanisms or SIS defined by expression (12) can be described by the expression

$$C(X) = \sum_{j=1}^{m} c_j x_j \tag{14}$$

In the final formulation of the task of optimizing the composition of the ISPS, we summarize the ideas presented by expressions (11), (13) and (14). Let it be necessary to determine the SIS, which will ensure compliance with the inequality $\tau \geqslant t_0 = T$, where $T > 0$ is the upper limit of the time interval during which the studied information system must be in functional state 0 despite the probable influence of the set ATIS I.

We limit the range of variation of the values of the characteristic parameters $R_i(X)$ to the boundaries of the domain of admissible solutions. The objective function is focused on the search in the set of SIS, which satisfies the newly formulated conditions, such that is characterized by minimal resource consumption:

$$C(X) = \sum_{j=1}^{m} c_j x_j \to \min \tag{15}$$

where

$$X = \left\{ X \in \{0,1\}^m ; \sum_{i=1}^{n} q_i R_i(X) \geqslant X^*(X^* - q_0) \right\} \tag{16}$$

where X^* is the desired SIS which is optimal according to (15) and satisfies constraint (16).

4. Results

Strictly proven correctness of the mathematical apparatus of Markov chains and transparency and reversibility of analytical transformations testify in favour of the adequacy of the method of operative optimization of the composition of ISPS presented in section 3. In the end, it remains to test the proposed method in real conditions. According to the previous agreement, the author had the opportunity to test the created method in a functioning information system for critical use of the Situational Center of the Information Technologies Department of Vinnytsia City Council.

The positive effect of the implementation of the method presented in Section 3 in the target information system is possible only after the analysis of operational data to determine the types of ATISs, the impact of which was recorded by ISPS. ATIS types were classified in the metrics proposed by the Open Web Application Security Project (OWASP). At https://owasp.org/www-project-top-ten/you can see a list of current ATIS types in order of danger. Analysis of logs information system of the Situation Center for the period from 01.09.2019 to 01.09.2021 revealed the facts of the impact of ATISs of types: A01:2021, A03:2021, A05:2021, A07:2021, A09:2021. The ratio of the revealed facts of ATIS implementation of each of these types to the total number of sessions of info-communication interaction for the censored period allowed to be embodied in the calculated set $Q = \{0.0296, 0.029, 0.038, 0.047, 0.048\}$. Visually, the results of the analysis of the impact of ATIS on the target information system for the censored period are presented in Fig. 2.

The structure of the ISPS information system of the Situation Center includes $R1$-Antivirus software; $R2$-Mechanism of protection of information from unauthorized access; $R3$-Hardware-software encryption mechanism; $R4$-Mechanism of data integrity control and recovery; $R5$-Author's mechanism for ISPS composition optimization. Resource-intensiveness of these protective mechanisms in c.u. generalized in the set $C = \{11.291, 8.157, 50.852, 8.906, 11.360\}$. The analysis of the contribution of each protective mechanism $R_i(X)$, $i = \overline{1,5}$, to the revealed facts of neutralization of ATISs of types A01:2021, A03:2021, A05:2021, A07:2021, A09:2021 for the censored period are presented in Fig. 3.

Therefore, all the necessary initial data for solving the optimization task of the form (15), (16) were obtained. Note that such a mathematical programming task can be classified as a nonlinear task of discrete programming. There is no one-size-fits-all method for solving such tasks. In modern operations theory, the method of complete search or the method of sequence variant analysis (SVA) is used to solve such optimization tasks [11]. The computational complexity of the solution process using the complete search method can be estimated in 2^m operations. For our particular case $m = 5$. But this approach is not technological.

We formalize the process of solving the optimization task (15), (16) by the SVA method. The most important thing is to determine a sufficient set of elimination tests $\sigma = \{\xi_0, \xi_1, \ldots\}$. Tests ξ_0 (checking the affiliation of the obtained solution to the domain of admissible solutions) and ξ_1 (comparison of the current solution with the previous one by the value of the objective function (15)) are mandatory.

Considering the non-descending nature of the function (15), we set the upper limit C_h for the value of intermediate solutions, $j \in J$, which will be equal to the best value of the objective function (15) determined on the set of calculated intermediate solutions: $\xi_2(h) = \{X_{(p)} \in h : j(X_{(p)}) > C_h\}$, where h is a subset of intermediate solutions from the domain. Thus, the set of elimination tests $\sigma = \{\xi_0, \xi_1, \xi_2\}$ is characteristic of the process of solving the optimization task (15), (16) by the SVA method.

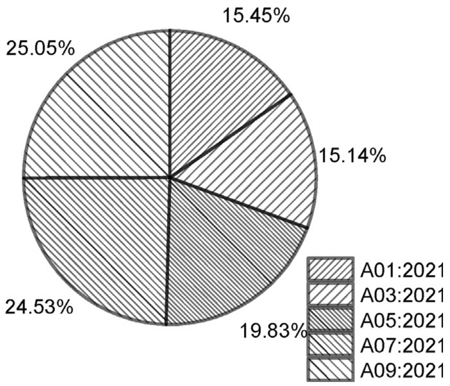

Fig. 2. Graphic interpretation of the set Q

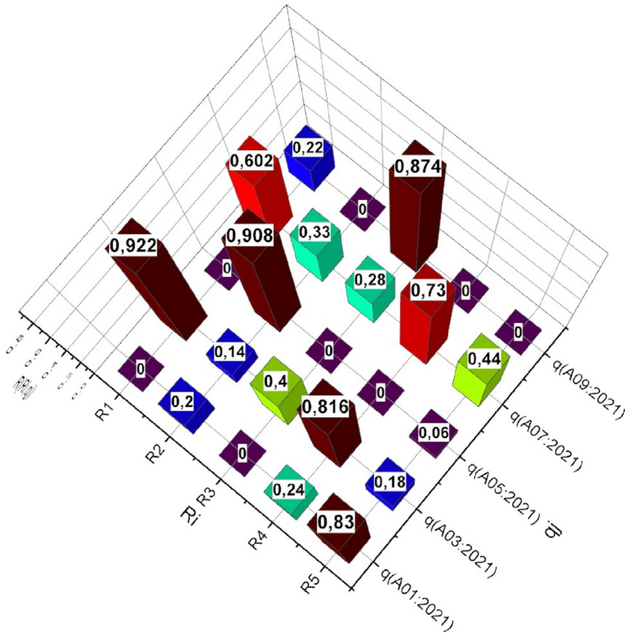

Fig. 3. The results of a preliminary analysis of the contribution of each protective mechanism to the neutralization of ATISs

We define a set of time points based on which we solve the optimization task (15), (16) by the SVA method for the information system of the Situational Center: $T = \{T_i = \lceil 0.05 i t_0 \rceil\}$, $i = \overline{1,4}$, where t_0 is the censored time for the studied information system, s. The result is the dependences $\{X^*, C^*\} = f\left(\left\{\overline{T_1, T_4}\right\}\right)$, which are presented in Fig. 4.

5. Discussion

Let's start the discussion with the statement shown in Fig. 4 fact that the optimization task (15), (16) for the studied information system had solutions for all investigated time intervals T_1/T_4. Considering that the time interval $t_0 \approx 6.307 \cdot 10^7$ s., this fact indicates that the structure of the ISPS generally corresponds to the degree of aggressiveness of the cyberspace in which the information system of the Situation Center operates. Recall that the system of constraints (16) was formed around the requirement (8), according to which with constant characteristics of ATIS (matrix (1)) the ISPS at the time T_i must provide the probability of the information system staying in state 0, which is not less than half the value of the probability that the information system is in state 0, calculated at the time of initiation of the operation process: $T_0 = 0$. This does not mean that the authors do not foresee a situation where there is no optimal solution for certain initial data. The condition of convergence of the process of solving the optimization task (15), (16) by the SVA method is the elimination rule ξ_1. If it is not executed on a certain iteration, the resolution process will stop with the corresponding verdict. By the way, due to the possibility of introducing an indicator of the lack of optimal solution, the authors preferred the SVA method over the method of complete search.

Now analyze the presented in Fig. 4 optimal results $\{X^*, C^*\} = f\left(\left\{\overline{T_1, T_4}\right\}\right)$. Note that in all sets X^* we see that $x_3 = 0$. This means that the $R3$ protective mechanism is not used to counteract the ATISs generalized be a set Q. Accordingly, it can be removed from the structure of ISPS without reducing confidentiality and increasing the availability of the studied information system.

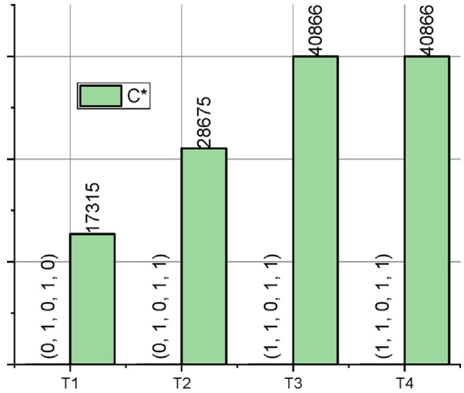

Fig. 4. The results of solving the optimization task (15), (16) for the studied information system: $\{X^*, C^*\} = f\left(\left\{\overline{T_1, T_4}\right\}\right)$

At the same time, with increasing value T, the expediency of the author's method of operative optimization of the composition of ISPS is confirmed experimentally – the protective mechanism $R5$ (Author's mechanism for ISPS composition optimization) is present in sets $X_2^* \div X_4^*$. Indirect confirmation of the adequacy of the proposed mathematical apparatus is that all optimal SIS include $R2$ and $R4$. Instead, the relevance of $R1$ is already manifested for long censored time intervals T_3, T_4. Oriented on the critical application of the studied information system, this situation is normal. In the first place are the issues of reliable user authentication and the integrity of information resources. Since the set of users of information resources and the list of services is strictly controlled, the need for anti-virus software manifests itself only over time. Mainly due to the need to control the processes and services of the information environment in which the researched information system operates.

Note that as the number of active defence mechanisms increases, the resource intensity of SIS increases (see Fig. 4). However, for a sufficiently large value T, even the activation of all protective mechanisms will not allow fulfilling conditions (8).

Finally, Fig. 3 shows that half of the failures recorded in the functioning of the studied information system were related to the problems of authentication and ensuring the stability of sessions of information interaction of users and the system. This fact again confirms the rationality of the presence of protective mechanisms $R2$ and $R4$ in all optimal SISs.

6. Conclusions

Increasing threats to the confidentiality and integrity of information require careful consideration of the problem of its protection. Traditional approaches to information security in the form of a composition of crypto-protection and access control mechanisms at the hardware and software levels are still effective for ordinary users. Instead, in the corporate sector, and even more so in the critical infrastructure sector, the capabilities of such composites are insufficient. This is confirmed by the constantly spreading information about successful hacker attacks. Thus, the problem of securing information that has financial, competitive, military or political value is extremely relevant.

However, increasing confidentiality should not forget about its antipode – availability. An effective information security protection subsystem must ensure a rational balance between the values of these dependability attributes. Analytically, this concept of balance can be embodied in the task of optimizing the values of the characteristic parameters of such a subsystem. At the same time, the concept of efficiency should be extended to such a mathematical apparatus. Its complexity should ensure the adequacy of the description of the information protection process but not be excessive to ensure that it can be applied. Based on these initial provisions, the article presents a method of operational optimization of the composition of the information security protection subsystem, taking into account the aggressiveness of cyberspace in which the target information system is operated. The method is formalized in the paradigm of Markov chains with the approach to the formulation of the classical optimization task, which is classified as nonlinear discrete. Considering the lack of a universal method for solving such mathematical programming tasks, the article adapts the method of sequential variants analysis for such purposes. The results of experiments proved the adequacy and functionality of the proposed method.

Further research is planned to take into account the possible dependence between artificial threats to information security. By "artificial threats" I mean hacker attacks, which, in contrast to, for example, DDoS attacks, have a thoughtful concept and implementation in manual mode. It is also promising to study the metrics for reliable identification of such threats.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The author would like to thank Arab Open University-Saudi Arabia for supporting this study.

References

[1] Colabianchi S, Costantino F, Di Gravio G, Nonino F, Patriarca R. Discussing resilience in the context of cyber physical systems. Comput Ind Eng 2021. doi: https://doi.org/10.1016/j.cie.2021.107534.

[2] Lallie HS, Debattista K, Bal J. A review of attack graph and attack tree visual syntax in cyber security. Computer Science Review 2020. doi: https://doi.org/10.1016/j.cosrev.2019.100219.

[3] George, P.G., Renjith, V.R., 2021. Evolution of Safety and Security Risk Assessment methodologies towards the use of Bayesian Networks in Process Industries. Process Safety and Environmental Protection. 10.1016/j.psep.2021.03.031

[4] Zhang L, Thing VLL. Three decades of deception techniques in active cyber defense – Retrospect and outlook. Computers & Security 2021. doi: https://doi.org/10.1016/j.cose.2021.102288.

[5] Bhamare D, Zolanvari M, Erbad A, Jain R, Khan K, Meskin N. Cybersecurity for industrial control systems: A survey. Computers & Security 2020. doi: https://doi.org/10.1016/j.cose.2019.101677.

[6] Iglesias Pérez S, Moral-Rubio S, Criado R. A new approach to combine multiplex networks and time series attributes: Building intrusion detection systems (IDS) in cybersecurity. Chaos, Solitons Fractals 2021. doi: https://doi.org/10.1016/j.chaos.2021.111143.

[7] Senarak C. Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel. The Asian Journal of Shipping and Logistics 2021. doi: https://doi.org/10.1016/j.ajsl.2021.10.002.

[8] Turk Ž, García de Soto B, Mantha BRK, Maciel A, Georgescu A. A systemic framework for addressing cybersecurity in construction. Autom Constr 2022. doi: https://doi.org/10.1016/j.autcon.2021.103988.

[9] van der Kleij R, Schraagen JM, Cadet B, Young H. Developing decision support for cybersecurity threat and incident managers. Computers & Security 2022. doi: https://doi.org/10.1016/j.cose.2021.102535.

[10] Delaval G, Hore A, Mocanu S, Muller L, Rutten É. Discrete Control of Response for Cybersecurity in Industrial Control. IFAC-PapersOnLine 2020. doi: https://doi.org/10.1016/j.ifacol.2020.12.2295.

[11] Švábenský V, Čeleda P, Vykopal J, Brišáková S. Cybersecurity knowledge and skills taught in capture the flag challenges. Computers & Security 2021. doi: https://doi.org/10.1016/j.cose.2020.102154.

[12] Cheung K-F, Bell MGH, Bhattacharjya J. Cybersecurity in logistics and supply chain management: An overview and future research directions. Transportation Research Part E: Logistics and Transportation Review. 2021. doi: https://doi.org/10.1016/j.tre.2020.102217.

[13] Jiang Y, Atif Y. A selective ensemble model for cognitive cybersecurity analysis. Journal of Network and Computer Applications 2021. doi: https://doi.org/10.1016/j.jnca.2021.103210.

[14] Ray A. Cybersecurity risk management-I. Cybersecurity for Connected Medical Devices 2022. doi: https://doi.org/10.1016/b978-0-12-818262-8.00005-x.

[15] Ray A. The Product Cybersecurity Organization. Cybersecurity for Connected Medical Devices 2022. doi: https://doi.org/10.1016/b978-0-12-818262-8.00011-5.

[16] Hong Y, Furnell S. Understanding cybersecurity behavioral habits: Insights from situational support. Journal of Information Security and Applications 2021. doi: https://doi.org/10.1016/j.jisa.2020.102710.

[17] Ogbanufe O, Kim DJ, Jones MC. Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. Information & Management 2021. doi: https://doi.org/10.1016/j.im.2021.103507.

[18] Yuan X, Liu S, Valdebenito MA, Faes MGR, Jerez DJ, Jensen HA, et al. Decoupled reliability-based optimization using Markov chain Monte Carlo in augmented space. Adv Eng Softw 2021. doi: https://doi.org/10.1016/j.advengsoft.2021.103020.

[19] Zhang Q, Liu Y. Reliability evaluation of Markov cyber–physical system oriented to cognition of equipment operating status. Comput Commun 2022. doi: https://doi.org/10.1016/j.comcom.2021.10.004.

[20] Wu B, Cui L. Reliability of multi-state systems under Markov renewal shock models with multiple failure levels. Comput Ind Eng 2020. doi: https://doi.org/10.1016/j.cie.2020.106509.

[21] Bisikalo, O., Chernenko, D., Danylchuk, O., Kovtun, V., Romanenko, V. 2020. Information Technology for TTF Optimization of an Information System for Critical Use that Operates in Aggressive Cyber-Physical Space. 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). 10.1109/picst51311.2020.9467997.

[22] Bisikalo OV, Kovtun VV, Kovtun OV, Danylchuk OM. Mathematical Modeling of the Availability of the Information System for Critical Use to Optimize Control of its Communication Capabilities. SWCC 2021. doi: https://doi.org/10.2174/2210327910999201009163958.

[23] Kovtun, V., & Izonin, I. (2021). Study of the Operation Process of the E-Commerce Oriented Ecosystem of 5Ge Base Station, Which Supports the Functioning of Independent Virtual Network Segments. In Journal of Theoretical and Applied Electronic Commerce Research (Vol. 16, Issue 7, pp. 2883–2897). MDPI AG. 10.3390/jtaer16070158

[24] Kovtun, V., Izonin, I., & Gregus, M. (2022). Model of Information System Communication in Aggressive Cyberspace: Reliability, Functional Safety, Economics. In IEEE Access (Vol. 10, pp. 31494–31502). Institute of Electrical and Electronics Engineers (IEEE). 10.1109/access.2022.3160837.

[25] Mahdavifar S, Ghorbani AA. Application of deep learning to cybersecurity: A survey. Neurocomputing 2019. doi: https://doi.org/10.1016/j.neucom.2019.02.056.