IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 7, 2022, accepted March 17, 2022, date of publication March 21, 2022, date of current version March 25, 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3160837*

# Model of Information System Communication in Aggressive Cyberspace: Reliability, Functional Safety, Economics

**VIACHESLAV KOVTUN[1], IVAN IZONIN[2], (Member, IEEE), AND MICHAL GREGUŠ[3]**
[1]Department of Computer Control Systems, Vinnytsia National Technical University, 21000 Vinnytsia, Ukraine
[2]Department of Artificial Intelligence, Lviv Polytechnic National University, 79013 Lviv, Ukraine
[3]Faculty of Management, Comenius University in Bratislava, 820 05 Bratislava, Slovakia

Corresponding author: Ivan Izonin (ivanizonin@gmail.com)

The National Research Foundation of Ukraine funded this research under the project "Neural network models, methods and tools for high-speed IoT data processing in information systems of critical application."

**ABSTRACT** The manuscript presents a mathematical apparatus for modeling the process of operation of the information system in the conditions of aggressive cyberspace, for which the corresponding parameter is provided. The highlight is that the simulation is carried out in the parametric space of reliability indicators, functional safety indicators, and economic indicators. The generalizing parameter in the mathematical apparatus is the coefficient of efficiency of operation of the studied system. It considers the accumulated parameter of efficiency of functioning of the studied system, the accompanying risk of its operation, and the number of resources invested in cybersecurity measures at its design stage. The connection of this coefficient with the probability of the information system transition to a non-functional state due to the realization of negative impact despite the resistance to cyber immune reaction is analytically described. The mathematical apparatus is developed to consider the errors of the first and second kind in identifying the negative impact on the information system. The search for the extreme value of the coefficient of the information system's efficiency from the number of resources invested in its cybersecurity measures is described considering the characteristic parameters of cyberspace in which the studied system is operated. The functionality of the created mathematical apparatus is demonstrated in the example of a study of a real information system of the Situational Center of the Department of Information Technologies of the Vinnytsia City Council (Ukraine). The results obtained showed that the amount of funds invested in cybersecurity at the design stage of the studied information system is sufficient for its operation in cyberspace, typical for the region. At the same time, the growth dynamics of the accumulated operational efficiency characteristics outpaces the growth dynamics of the characteristics of the risk of studied information system operation. The simulation results coincide entirely with the empirical experience of the studied system operation, which allows us to recognize the created mathematical apparatus as adequate. The simulation showed that when the value of the probability of incorrect identification of the negative impact level intersects the value of ≈0.007, the studied system operational efficiency coefficient begins to decline rapidly. It indicates that the amount of resources invested in cybersecurity of the studied information system is exhausted.

**INDEX TERMS** Cybersecurity, information system, negative impact, operation process, mathematical model, efficiency, reliability, functional safety.

## I. INTRODUCTION

The website of the well-known analytical company *Canalys* presents the research results, according to which the global cybersecurity market in 2021 will increase by 6-10% and amount to $57-60 billion, respectively. The company's specialists segmented the cybersecurity market into such clusters as endpoint security, network security, information systems security, information resources security, vulnerability search, and analysis. According to the forecast, the fastest growth is expected in the information systems security cluster (12.5%) and the vulnerability search and analysis cluster (11%). This

The associate editor coordinating the review of this manuscript and approving it for publication was Cheng Qian.

information is the best proof of the relevance of the investigation. This manuscript presents the results directly related to the first of the above clusters and indirectly – to the second.

Among the existing classes of information systems, a special place is occupied by the so-called information systems for critical use [1]–[3]. The operation of such systems is characterized by specific requirements for determining the attributes of dependability; the condition for maintaining the predicted trend of variation of the values of these attributes during the system's operation [4]–[6]. It is due to counteraction mechanisms to the cyber threats laid down at the design stage. The most characteristic structural units of such a subclass of information systems are:

- an information resources managed by an object-relational database management system that controls their integrity;
- an information environment that implements only a set of services defined at the design stage of the system, including support for the interface of the user-system interaction. Implementation of relevant services takes place exclusively in dedicated information processes with integrated control of integrity and confidentiality;
- the cyber security subsystem, which manages confidentiality and reliability levels due to protection mechanisms, taking into account the current resource consumption of the functional state of investigated information system by the rules of security policy.

A distinctive feature of the information systems for critical use is reliable predictability of all information processes provided by adequate profile mathematical models with the ability to calculate the values of dependability as a system in general and its components in particular.

Of course, the information capacity of the process of the operation of the information systems for critical use in the complete metric of attributes of dependability significantly exceeds the allowable size of the article, so in this research, we focus on such attributes as

- the reliability, which characterizes the ability of the studied system to retain its functional purpose in full despite the influence of cyber threats;
- the functional safety, which characterizes the ability, which is extremely important for information systems for critical use, to go into a non-functional state without significant material or human losses in the defeat of a cyber threat.

However, obtaining such models in a general form is a topical but theoretical task. For their practical application, it is necessary to introduce parameters into the created mathematical apparatus that characterize the information system under study in the economic field. Surprisingly, this obvious fact has not yet been reflected in the existing mathematical models of the functioning of information systems in the conditions of cyber aggression. However, this circumstance will be analyzed in more detail later. The ***research challenge*** of investigation is the process of operation of the information system in the conditions of aggressive external cyberspace. The ***aim*** of the study is the analytical formalization of this process in the parametric space of indicators of reliability, functional safety, economic efficiency, and taking into account the potential impact of negative factors.

The most pressing issue in cybersecurity is identifying and describing unfavorable impacts or cyber threats. The reliable result of their identity is the basis for the rational choice of methods and means of their disposal. Let us mention only the generally accepted methodologies used to estimate the state of cybersecurity, modeling of means of protection of information resources, and identification of negative impacts on information systems. These are [4], [5], [7]–[9]: game theory, fuzzy sets, graph theory, Petri nets, digital automata theory, random process theory, and so on.

These methodologies form a toolkit for analyzing the performance of the studied information systems for a finite censored period. The analysis takes place in the context of determining:

1. The time between failures in the studied system;
2. The number 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 response of the studied system to complex test effects.

Models [10]–[13] focused 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 data sample that characterizes the studied system's operation. When formalizing such models, only the failure is taken into account without analyzing the causes of its occurrence and possible consequences.

Models [14]–[17] focused on the description of the second performance indicator. It is assumed that a specific distribution law (most often Poisson's) with a continuous or discrete intensity function describes the stochastic parameter, which characterizes the number of time failures. 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 [18]–[21] focused 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 was caused by unknown negative impacts;
- the number of failures in the operation of the studied system during the censored period, which was 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 were collected because of uncontrolled experiments.

Models [1], [2], [22]–[24] focused 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 [25]–[27]. This allows considering the multithreading in the operation of the studied system and the heterogeneity of the process of its recovery after a failure. Semi-Markov models more accurately describe the behavior of real information systems because the process of recovery of the first ones after failures can be characterized not only by the exponential distribution functions [28]. The structural features of the studied system in this modeling approach can be considered 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, a nonparametric neural network [17], [29], [30], in which the structural 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 analogs are the models of information systems confidentiality based on discrete Markov chains described in paper [1], [2], [22]–[24]. The mentioned reliability models are classified as parametric. At the same time, there are nonparametric models built, for example, based on artificial neural networks [31], [32], which allow approximating arbitrary nonlinear continuous functions with the required accuracy [33], [34]. However, when synthesizing such models, the structural features of the system under study are not considered, and the accuracy of the resulting models is determined mainly by the type, architecture, and specifics of the learning process of the neural network used by the researcher [35].

Considering the above, the optimal from the standpoint of taking into account the architectural features of the information systems for critical use and the specifics of its functioning is the construction of models for estimation its reliability based on the mathematical apparatus of Markov chains. Close analogs are the models of confidentiality of information systems described in papers [15], [23], [31]–[33], formalized based on discrete Markov chains. These models are based on the theory of reliability elements and describe the studied information system as a system with failures and restorations.

The strength of these studies is the mathematically correct stochastic characteristic of the states of the studied system and a particular functional relationship between the estimate of the confidentiality of the studied system and the relaxation time of the Markov chain. However, even the specialized applied usage of the scientific results mentioned in articles [36]–[38] will be accompanied by significant complications because they ignore the potential impact of complex cyber threats on the studied system, which contradicts the realities of modern cyberspace.

Also, the finite parametric space used in the mentioned studies characterizes the studied systems exclusively in terms of the classical theory of probability and mathematical statistics and not the theory of dependability or reliability. And, in general, in the mentioned studies, the scope of application of the investigated information systems is wholly ignored. For example, in general-purpose information systems, it is allowed to narrow the range of functional services to improve survivability. Still, this approach is unacceptable in information systems for critical use. It is the basis for initiating a safety protocol for the safe transfer of such an information system to a non-functional state.

In [4], the authors, in terms of Markov chains with discrete-time, described the process of functioning of the information systems for critical use under the influence of certain negative factors on it. In this research, by analogy with the models of technical systems in terms of the theory of reliability, the information system for critical use is presented as a system with failures and restorations. In [1], [2], [22]–[24], the authors have developed this model to formulate the task of finding the optimal superposition of settings the protection means of information systems for critical use, depending on the characteristics of independent certain negative factors affecting it. But the economic component of preparing the target information system for operation and supporting this process has not yet been described at the proper theoretical level.

The ***object*** of investigation is the process of operation of the information system in the conditions of aggressive external cyberspace. The ***aim*** of the study is the analytical formalization of this process in the parametric space of indicators of reliability, functional safety, economic efficiency, and taking into account the potential impact of negative factors. So, the ***main contributions*** of this article are as follows:

— we have created mathematical apparatus for modeling the process of operation of the information system in the conditions of aggressive cyberspace in the parametric space of reliability indicators, functional safety indicators, and economic indicators such as profit from the intended use of the studied system and inflation and discount rates;
— to assess the readiness of the target information system for operation under appropriate conditions of cyberspace at the design stage, the corresponding parameter is expressed in the proposed mathematical apparatus – the coefficient of efficiency of operation of the studied information system;
— we formulated the task of finding the optimal value of the coefficient of efficiency of operation of the studied information system;
— we have provided an example of calculating all the characteristic parameters of the created mathematical apparatus on the real object – the Situation Centre of the

Department of Information Technologies of Vinnytsia City Council (Ukraine).

## II. MATERIALS AND METHODS

### A. STATEMENT OF THE RESEARCH

Let the studied information system (RIS) interact with the aggressive external cyber-physical space in the process of operation. The aggressiveness of cyberspace is manifested in the non-periodic negative impacts of external factors of man-made or device-made origin. The realization of such a negative impact on the DIS is estimated by the stochastic value $q$ and can cause the latter's transition to a non-functional state $S_{off}$. The stochastic parameter characterizes the probability of such an event $\pi$, and the losses suffered by RIS in the event of premature interruption of the operation process are determined by the parameter $d_0$. The RIS reliability level will be characterized by the failure rate $\lambda(t)$, and the intensity and efficiency with which it realizes its functional purpose will be denoted by the parameters $\mu(t)$ and $w_0$, respectively. The parameter $w_0$ characterizes the cumulative profit that provides a functioning RIS from the moment of initiation of the operation process. The ability of RIS to counteract the impact of negative factors is laid at the stage of its design and is characterized by the amount of invested resources $C$. Accordingly, the function can describe the effectiveness of the RIS cyber immune response to possible negative impact $\pi(C)$.

Taking into account the introduced basis, we formulate the ***objectives*** of the investigation:

1) to formalize a practice-oriented model of the RIS operation process in aggressive cyber-physical space;
2) to prove the adequacy of the proposed model and test it to describe the operation of a real information system.

### B. MATHEMATICAL MODEL OF THE STUDIED PROCESS

Let us redefine for any moment $t > 0$ the characteristic parameters of efficiency and losses, taking into account the determined coefficients of inflation $r$ and discounting $i$:

$$d(t) = d_0 \gamma^t \tag{1}$$

where $\gamma = (1+r)/(1+i)$ and $t = 0$ is the moment of the beginning of operation of RIS.

We characterized by the parameter $p_0(t)$ the probability that at time $t > 0$ RIS is in the functional state $S_{on}$. Let us represent this stochastic parameter in dynamics by an equation:

$$dp_0(t)/dt = -p_0(t) \times (q\pi\mu(t) + \lambda(t)) \tag{2}$$

By analogy with (2), we present in the dynamics of the accumulated parameter of the efficiency of RIS $W(t)$:

$$dW(t)/dt = -p_0(t) \times (1 - q\pi) w(t) \tag{3}$$

and associated risk of its operation $R(t)$:

$$dR(t)/dt = p_0(t) \times q\pi\mu(t) d(t) \tag{4}$$

The ratio of indicators (3), (4) rationally characterizes the process of RIS operation in the conditions of aggressive cyberspace if we additionally take into account the cyber immune potential $C$ laid down at the stage of its design: $\beta(t) = W(t)/(R(t) + C)$. If we postulate the independence of the parameters $\mu(t)$ and $\lambda(t)$, then the solution of equation (2) in analytical form is defined as

$$p_0(t) = \exp(-t(q\pi\mu + \lambda)) \tag{5}$$

Express in analytical form the solution of expressions (3) and (4) taking into account the dependence (1) and solution (5):

$$W(t) = \frac{\mu w_0 (1 - q\pi)}{\ln\gamma - (q\pi\mu + \lambda)} (\exp(t(\ln\gamma - (q\pi\mu + \lambda))) - 1) \tag{6}$$

$$R(t) = \frac{q\pi\mu d_0}{\ln\gamma - (q\pi\mu + \lambda)} (\exp(t(\ln\gamma - (q\pi\mu + \lambda))) - 1) \tag{7}$$

Mathematical analysis of expressions (6) and (7) suggests that when the condition:

$$\ln\gamma - (q\pi\mu + \lambda) < 0 \tag{8}$$

the limit values of the parameters $W$ and $R$ are determined by the corresponding expressions:

$$W_{\lim} = \frac{\mu w_0 (1 - q\pi)}{(q\pi\mu + \lambda) - \ln\gamma}, \quad R_{\lim} = \frac{\mu d_0 q\pi}{(q\pi\mu + \lambda) - \ln\gamma}.$$

If condition (8) is satisfied, the value of the coefficient $\beta(t)$ will increase, but in general, will not exceed the limit value

$$\beta^-_{\lim} = \frac{w_0 (1 - q\pi)}{C(q\pi\mu + \lambda)/\mu + q\pi d_0} \tag{9}$$

If condition (8) is not fulfilled, then the value of the coefficient $\beta(t)$ will still increase, but in general, will not exceed the limit value:

$$\beta^+_{\lim} = \frac{w_0 (1 - q\pi)}{q\pi d_0} \tag{10}$$

By the way, condition (8) may not be fulfilled only if the discount rate $i$ is lower than the inflation rate $r$:

$$i < r \tag{11}$$

For the RIS operating in conditions (11) to be in the $S_{on}$ state, it is necessary to set such an amount of resource $C$ at the design stage that the inequality $\pi(C) < (-\lambda + \ln\gamma)/\mu q$ is satisfied for the value of the probability of RIS transition to the $S_{off}$ state as a result of realization of the negative impact $\pi(C)$.

We now describe the behavior of RIS in a situation where condition (11) is not satisfied. Rewrite expression (9):

$$\beta^-_{\lim}(C) = \frac{w_0 (1 - q\pi(C))}{C(\lambda - \ln\gamma)/\mu + q(C + d_0)\pi(C)} \tag{12}$$

We obtain the analytical form of the derivative of the parameter (12):

$$\frac{d\beta^-_{\lim}(C)}{dC}$$

$$= \frac{-w_0 q\,(C + d_0 + (C\,(\lambda - \ln\gamma))/\mu)\,\pi'\,(C)}{((C\,(\lambda - \ln\gamma))/\mu + q\,(C + d_0)\,\pi\,(C))^2} + \frac{w_0 q\,(q\pi\,(C) + (\lambda - \ln\gamma)/\mu - 1) - (\lambda - \ln\gamma)/\mu}{((C\,(\lambda - \ln\gamma))/\mu + q\,(C + d_0)\,\pi\,(C))^2}. \quad (13)$$

From expression (13), it is seen that the numerator of the function $d\beta_{\lim}^{-}(C)/dC$ is a quadratic function concerning the parameter $\pi\,(C)$. Therefore, if one of the roots of the function (13) belongs to the interval [0, 1], then the extremum of the function $\beta_{\lim}^{-}(C)$ exists. Let us present this statement analytically:

$$q^2\pi^2 + (((\lambda - \ln\gamma)/\mu - 1)\,\pi - q\,(d_0 + C + (C\,(\lambda - \ln\gamma))/\mu)\,\pi' - (\lambda - \ln\gamma)/\mu = 0 \quad (14)$$

To simplify equation (14), we assume that the dependence $\pi\,(C)$ has an exponential character: $\pi\,(C) = \exp(-\xi C)$, where the coefficient $\xi > 0$ characterizes the effect of investing in cybersecurity of RIS several resources equal to $C$. Let us refine expression (14), taking into account the just presented interpretation of the function $\pi\,(C)$:

$$q^2\pi^2 - \pi\,(1 - (\lambda - \ln\gamma)/\mu - q\xi \times (d_0 + C + (C\,(\lambda - \ln\gamma))/\mu)) - (\lambda - \ln\gamma)/\mu = 0. \quad (15)$$

We present expression (15) in a compact form:

$$q^2\pi^2 - s\pi - b = 0 \quad (16)$$

where $s = 1 - (\lambda - \ln\gamma)/\mu - q(d_0 + C + (C(\lambda - \ln\gamma))/\mu)\xi$, $b = (\lambda - \ln\gamma)/\mu$. The positive root of such an equation is defined as:

$$\pi = \left(s + \sqrt{s^2 + 4bq^2}\right)\Big/ 2q^2 \quad (17)$$

Based on the fact of existence and value of the parameter $\pi$, defined by expression (17), we can estimate how much resources embedded in the design phase of RIS in its cyber immune potential $C$ corresponds to the real level of aggressiveness of cyberspace where RIS is operated $\beta\,(t)$.

Based on the starting points of our investigation, it can be stated that if the realized negative impact is not identified, then its activity is guaranteed to cause the transition of RIS to state $S_{off}$. In turn, the cyber immune potential laid down at the RIS design stage allows neutralizing it with probability $q$ in case of identification of negative impact. The above analytical concept does not consider that the negative impact can be identified incorrectly (error of the first kind), so we introduce a stochastic parameter $f$, which characterizes the probability that the implemented RIS will correctly identify negative impact. The information system using these parameters may transit into the state $S_{off}$ as a result of the negative impact if: - the negative impact is not identified: $1 - f$; - negative impact identified but not neutralized: $\pi f$. Based on this information, we rewrite equation (2)-(4):

$$\frac{dp_0\,(t)}{dt} = -p_0\,(t) \times (q\mu\,(t)\,(1 - f\,(1 - \pi)) + \lambda\,(t)), \quad (18)$$

$$\frac{dW\,(t)}{dt} = p_0\,(t) \times (1 - q + qf\,(1 - \pi))\,\mu\,(t)\,w\,(t) \quad (19)$$

$$\frac{dR\,(t)}{dt} = p_0\,(t) \times q\,(1 - f\,(1 - \pi))\,\mu\,(t)\,d\,(t) \quad (20)$$

The introduction of the parameter $f$ is the basis for rethinking the method of taking into account the losses $d_0$ suffered by RIS in the event of premature interruption of the operation process. We introduce the following indicators: $d_1$ is the losses caused by the implementation of the negative impact, as a result of which RIS transit into the state $S_{off}$ in compliance with the protocol of functional safety; - losses caused by the implementation of the negative impact, as a result of which RIS uncontrollably transit to state $S_{off}$ (emergency). We introduce these indicators in equation (20):

$$\frac{dR\,(t)}{dt} = p_0\,(t) \times q\,(f\,(1 - \pi)\,d_1 + (1 - f + \pi f)\,d_2)\,\mu\,(t)\,\gamma^t \quad (21)$$

Model (18), (19), (21) still does not fully describe the actual process of RIS exploitation in aggressive cyber-physical space. In particular, when examining the issue of identifying negative impacts, one cannot ignore the probability of the occurrence of errors of the second kind, i.e., situations when the target cyber immune reaction is a consequence of identifying negative impact, which was not realized. It should be borne in mind that the targeted use of RIS is impossible during a cyber immune reaction. To take into account the situation just described, we expand the state space of RIS: $S = \{S_{on}, S_1, S_2, S_{off}\}$, where: - $S_{on}$ is the state of readiness, in which the functioning RIS is waiting for an incoming request, which comes with intensity $\mu\,(t)$. The probability of RIS being in state $S_{on}$ is characterized by the parameter $p_0\,(t)$;

- $S_1$ is the state of processing the received request, which is carried out with intensity $v\,(t)$. The probability of RIS being in state $S_1$ is characterized by the parameter $p_1\,(t)$;
- $S_2$ is the state of the active cyber immune response during which the target security policy protocol is executed with intensity $\phi\,(t)$.

The parameter characterizes the probability of RIS being in the state $p_2\,(t)$; - $S_{off}$ is a state in which RIS does not function. The probability of RIS being in state $S_{off}$ is characterized by the parameter $p_3\,(t)$. States $S_{on}$ and $S_1$ are functional because being in them, RIS realizes its purpose. Accordingly, the states $S_2$ and $S_{off}$ are non-functional.

Let the negative impacts be realized with intensity $\eta\,(t)$. Suppose that the fixed negative impact is an imitation. We characterize such an event by probability $l_0$. Denote by the identifier $f_0$ the probability of correct identification of the imitation of the negative impact, and by the identifier $f_1$ the probability of the correct identification of the negative impact. In sum, these parameters characterize the probability of correct identification of negative activity. We will not change the interpretation of the RIS failure rate $\lambda\,(t)$ and the probability of the system transitioning to a non-functional state as a result of the negative impact $\pi$. Limited by the

state space $S$, the dynamics of the RIS operation process is determined by the equations:

$$\frac{dp_0(t)}{dt} = p_0(t) \times (-\mu(t)) + p_1(t) \times v(t), \quad (22)$$

$$\frac{dp_1(t)}{dt} = p_0(t) \times \mu(t) + p_2(t) \times \phi(t)(1-\pi(1-l_0)) - p_1(t) \times (\lambda(t) + v(t) + \eta(t)(1-f_0 l_0)), \quad (23)$$

$$\frac{dp_2(t)}{dt} = p_2(t) \times (-\phi(t)) + p_1(t) \times \eta(t)(f_1(1-l_0) + l_0(1-f_0)), \quad (24)$$

$$\frac{dp_3(t)}{dt} = p_2(t) \times (\phi(t)\pi(1-l_0)) + p_1(t) \times (\lambda(t) + \eta(t)(1-f_1)(1-l_0)), \quad (25)$$

$$dW(t)/dt = p_1(t) \times w(t) v(t), \quad (26)$$

$$\frac{dR(t)}{dt} = d_1 \times p_2(t)\phi(t)(1-f_1)(1-l_0)\gamma^t + d_2 \times (p_1(t)\eta(t)(1-\pi)(1-l_0) + p_2(t)\phi(t)\pi(1-l_0))\gamma^t. \quad (27)$$

Determine the analogues of equations (3) and (4), taking into account the fact of the existence of equations (22)-(25)):

Equations (23) and (26) can be simplified if we assume that RIS is operated continuously. In accordance:

$$\frac{dp_1(t)}{dt} = p_1(t) \times -(\eta(t)(1-f_0 l_0) + \lambda(t)) + p_2(t) \times \phi(t)(1-\pi(1-l_0)),$$

$$dW(t)/dt = p_1(t) \times w(t).$$

The assumption made does not affect equations (24), (25), (27).

## III. MODELING AND RESULTS

Strict correctness and reversibility of analytical transformations testify in favour of the adequacy of the mathematical apparatus presented in Section 3. In the end, it remains to test it in real conditions. According to the previous agreement, the authors had the opportunity to test the created mathematical apparatus by describing the operation of the real information system of the Situation Centre of the Department of Information Technology of Vinnytsia City Council. This information system has been operating since 2018 and is constantly evolving to improve the implemented services and add new ones. In particular, the information system of the Situation Centre manages traffic lights on the city roads. It supports the uninterrupted operation of the data center, which stores the flow of multimedia data from more than 1k video cameras located in the city. Only authorized employees of the Security Service of Ukraine, the National Police of Ukraine, Vinnytsia City Council, etc., have access to the collected confidential information. Considering the intensity of information exchange and the nature of information resources, the issue of modeling the operation of this RIS is extremely relevant.

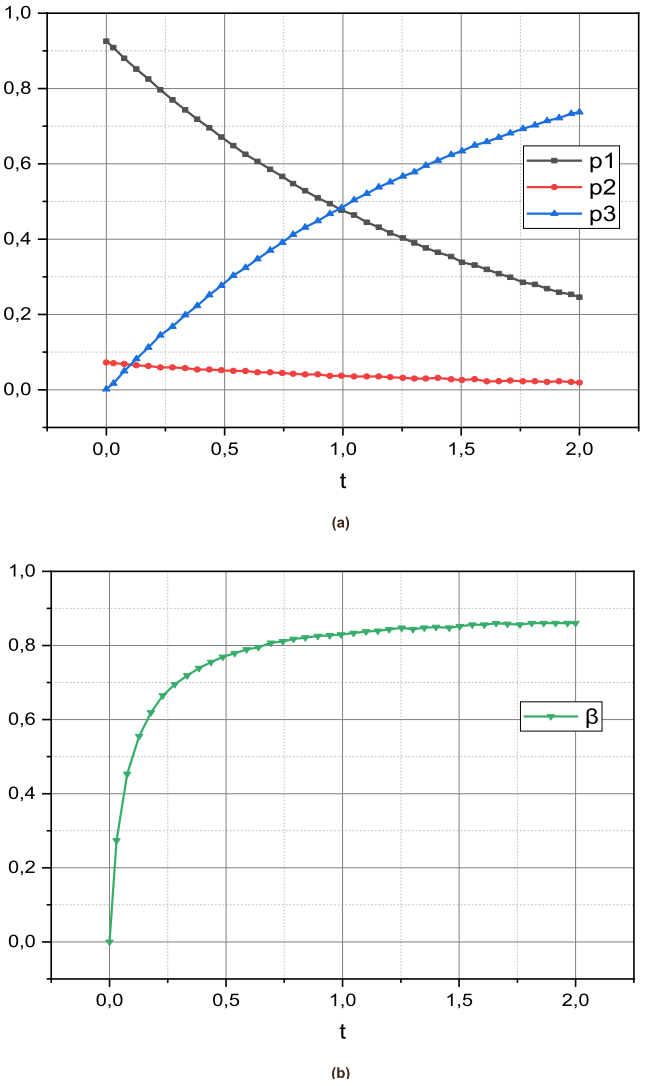


**FIGURE 1.** (a) Empirical dependencies $\{p_1, p_2, p_3\} = f(t)$. (b) Empirical dependencies $\beta = f(t)$.

We will perform RIS modeling in the state space $S = \{S_{on} = \{S_{on}, S_1\}, S_{off} = \{S_2, S_{off}\}\}$. to make this section sufficiently compact. Analysis of RIS continuous operation logs from 01.09.2019 to 01.09.2021 in the context of the selected state-space configuration allowed us to determine the following values of the established parameters of the created model: $\lambda = 10^{-5}$, $\pi = 0.01$, $r = 0.05$, $i = 0.1$, $\eta = 5$, $\phi = 50$, $f_0 = f_1 = 0.99$, $d_0 = 0.1$, $d_1 = 10$, $l_0 = 0.2$, $w_0 = 1$. As a starting value, we take $C = 1$. Substituting these parameters into expressions (23)-(26), we performed a simulation of dependencies $\{p_1, p_2, p_3\} = f(t)$, $\beta = f(t)$ for RIS. The corresponding results are presented in the graphs in Fig. 1(a), 1(b).

Based on the calculations, the results of which are visualized in Fig. 1, based on expressions (26) and (27) for RIS the dependencies $\{W, R\} = f(t)$ are calculated, where $W$ is the accumulated parameter of efficiency of operation of RIS, and $R$ is the accompanying risk from its operation. The corresponding graphs are shown in Fig. 2.

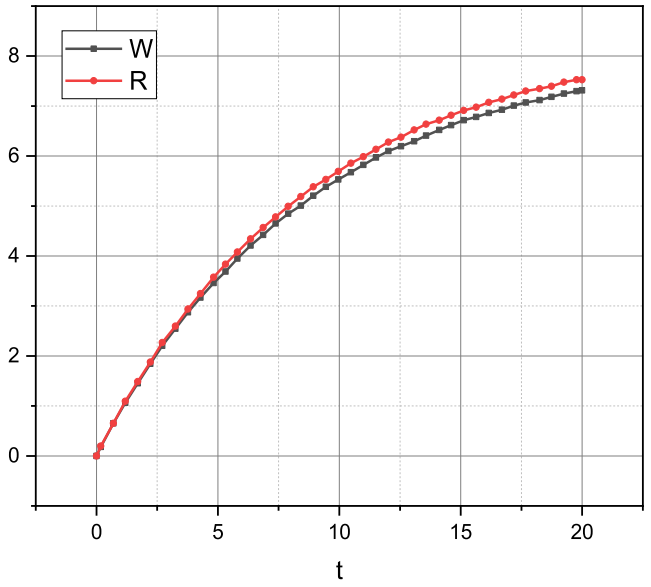


**FIGURE 2.** Empirical dependencies $\{W, R\} = f(t)$.

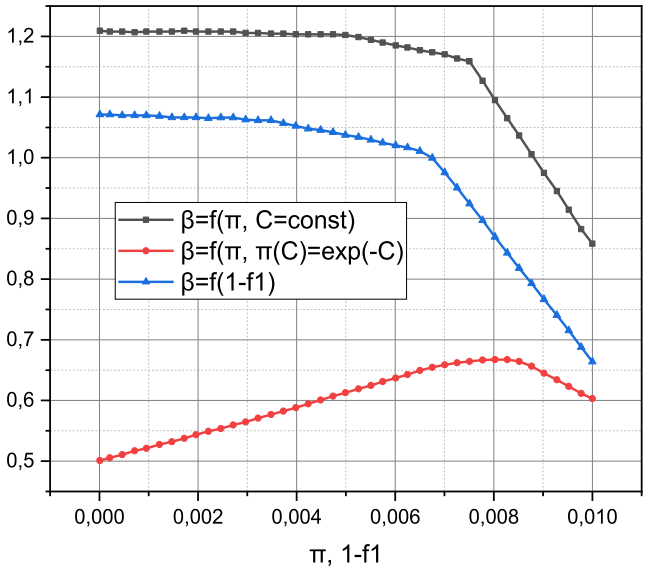


**FIGURE 3.** Empirical dependencies $\beta = f(\pi, C = \text{const})$, $\beta = f(\pi, \pi(C) = \exp(-C))$, $\beta = f(1 - f_1)$.

Finally, the central issue of our investigation is to establish the fact: we're the investments into the cyber immune system at the RIS design stage $C$, taking into account the level of cyberspace aggression represented by the value of the parameter $\pi$ sufficient? To answer this question, a series of experiments was performed to calculate the dependences of $\beta = f(\pi)$ for $\pi(C) = \text{const}$ and $\pi(C) = \exp(-C)$. It will be recalled that $\beta = f(W, R, C)$ is a generalized efficiency coefficient of RIS in terms of the fulfillment of its intended purpose in real operating conditions.

Since condition (11) was not satisfied for our RIS, the dependences $\beta = f(\pi)$ were calculated by expression (13). Also relevant is objective information on the calculation for the RIS, the dependence of $\beta = f(1 - f_1)$ where $f_1$ is the probability of correctly identifying the negative impact. This dependence characterizes the ability of the cyber immune system of RIS to neutralize the detected but incorrectly identified negative impacts. The graph representing the dependence $\beta = f(1 - f_1)$ for $\pi = 0.005$ calculated RIS is also shown in Fig. 3.

We generalize the experimental section by verifying the models proposed in Section 3 in the paradigm of practical planning theory. We form certain sets of input influences, the appearance of which can cause the loss of functioning: $X^k = \{x_1^k, x_2^k, \ldots, x_n^k\}$ and $X^{\bar{k}} = \left\{x_1^{\bar{k}}, x_2^{\bar{k}}, \ldots, x_m^{\bar{k}}\right\}$. The system's response to input effects from the set $X^k$ is predicted in the model. Therefore, under such conditions, the studied information system should not fall. Input influences from the set $X^{\bar{k}}$ are structurally identical to the generalized set $X^k$ but differ in values that may exceed the limits set up at the system's design stage. The system's reaction to the input influence from the set $X^{\bar{k}}$ can be the fall into an unfunctional state. The numbers of elements in the sets $X^k$ and $X^{\bar{k}}$ are $n = 200$ and $m = 700$, respectively. Experiments were performed with a fixation on the system's reaction to the input influences from the sets $X^k$ and $X^{\bar{k}}$ (in the matrix form $B_e^k = \left(B_{ij}^k\right)$, $i = \overline{1, n}$, and $B_e^{\bar{k}} = \left(B_{ij}^{\bar{k}}\right)$, $i = \overline{1, m}$, respectively). We calculate for the $i$th input influence the variance of the implementation of the situation of the fall of a studied system into the unfunctional state: $s_i^2 = M^{-1} \sum_{j=1}^{M} \left(B_{ij} - B'_{ij}\right)^2$, where $B_{ij}$ is the state defined in the model; $B'_{ij}$ is the actual state. We calculate the average value of the variance for all input influences: $s^2 = N^{-1} \sum_{i=1}^{N} s_i^2$. Evaluation of the substantial deviations $s_i^2$ from $s^2$ Fisher's criterion showed that all deviations do not exceed the tabular values, which confirms the adequacy of the proposed mathematical apparatus.

## IV. DISCUSSION

Let's start the discussion with the analysis of graphs from Fig. 1. Recall that the parameters $p_1(t), p_2(t), p_3(t)$, characterize the probabilities of RIS at a time $t$ in one of the states $S_1$, $S_2$, $S_{off}$, respectively. Of these, the state $S_1$ is functional. A state $S_2$ corresponds to an active cyber immune response, and a state $S_{off}$ describes a situation where RIS is prematurely decommissioned due to the implementation of a negative impact. Dependences $\{p_1, p_2, p_3\} = f(t)$ with increasing value $t$ uniquely reproduce the real dynamics of the operation of DIS: $p_1(t)$ decreases, and $p_2(t)$ on the contrary, increases. The fact that $p_3(t)$ is slowly declining indicates a surplus of the number of resources invested in cybersecurity of RIS $C$. However, with the increasing probability of negative impact, the coefficient of RIS operational efficiency $\beta$ is still increasing because the graph $p_2(t)$ is also increasing. As shown in Fig. 2, dependences $\{W, R\} = f(t)$ also confirm the adequacy of the number of resources invested in cybersecurity of RIS. This statement is true because the growth dynamics of the accumulated RIS operational efficiency characteristics

$W$ outpaces the growth dynamics of the characteristics of the risk of its operation $R$.

In general, the nonlinear exponential nature of the dependencies in Figs. 1 and 2 confirm the correctness of assumption (5), and the fact that the RIS operational efficiency ($\beta = f(t)$) increases even though according to the initial conditions of the experiment, the inequality (11) is not satisfied, corresponds to equation (12). As shown in Fig. 1 and 2, the results of the simulation completely coincide with the empirical experience of the RIS operation, which allows us to recognize the mathematical apparatus presented in Section 3 as adequate.

Let's pay attention to Fig. 3. It is seen that when the value of the probability of incorrect identification of the negative impact level $1 - f_1$ intersects, the value of $\approx 0.007$ the RIS operational efficiency coefficient $\beta$ begins to decline rapidly. This indicates that the amount of resources invested in cybersecurity of RIS $C$ is exhausted. This statement correlates with the dynamics shown by the graph $\beta = f(\pi, C = \text{const})$ and generally confirms the correctness of the created mathematical apparatus. Finally, the visible extremum on the graph $\beta = f(\pi, \pi(C) = \exp(-C))$ and the same form of this dependence corresponds to the logic of mathematical concepts embodied in expression (17). However, the question of determining the optimal amount of resources $C$ invested at the design stage of RIS in cybersecurity of the latter should be investigated in a full-size parametric space $\{\pi, l_0, f_0, f_1\}$, which is a promising area of further research.

Finally, it should be noted that the mathematical apparatus for modeling the process of operation of the information system in the conditions of aggressive cyberspace proposed in the article is proved to be adequate because it is based on the verified mathematical apparatus of Markov chains. This fact and the rigor and reversibility of the analytical transformations made in the formalization of the corresponding metric substantiate the adequacy of the mathematical apparatus presented in the article.

## V. CONCLUSION

Information systems are designed to meet the primary need of modern man – access to data recourses. Investigations aimed at improving the quality of services for such systems is undeniably actual.

The manuscript presents a mathematical apparatus for modeling the process of operation of the information system in the conditions of aggressive cyberspace, for which the corresponding parameter is provided. Unlike analogs, the simulation is carried out in the parametric space of reliability indicators, functional safety indicators, and economic indicators such as profit from the intended use of the studied system and inflation and discount rates. The generalizing parameter in the mathematical apparatus is the coefficient of efficiency of operation of the studied information system. It considers the accumulated parameter of efficiency of operation of the studied system, the accompanying risk of its operation, and the number of resources invested in cybersecurity measures at its design stage. The connection of this coefficient with the probability of transition of the information system to a non-functional state due to the realization of the negative impact despite the resistance to the cyber immune reaction is analytically described. The mathematical apparatus is developed to take into account the errors of the first and second kind in identifying the negative impact on the information system. The case when the cyber immune reaction to the imitation of negative impact is investigated separately. The search for the extreme value of the coefficient of efficiency of the information system from the number of resources invested in its cybersecurity measures is described considering the characteristic parameters of cyberspace in which the studied system is operated. The investigation of the real information system of the Situation Centre of the Department of Information Technologies of Vinnytsia City Council led to the adequacy of the proposed mathematical apparatus.

***Further research*** is planned to focus on detailing the parametric space of finding the extreme value of the coefficient of efficiency of operation of the RIS.

## REFERENCES


[1] O. Bisikalo, D. Chernenko, O. Danylchuk, V. Kovtun, and V. Romanenko, "Information technology for TTF optimization of an information system for critical use that operates in aggressive cyber-physical space," in *Proc. IEEE Int. Conf. Problems Infocommun. Sci. Technol. (PIC S&T)*, Kharkiv, Ukraine, Oct. 2020, pp. 323–329, doi: 10.1109/PICST51311.2020.9467997.

[2] O. V. Bisikalo, V. V. Kovtun, O. V. Kovtun, and O. M. Danylchuk, "Mathematical modeling of the availability of the information system for critical use to optimize control of its communication capabilities," *Int. J. Sensors, Wireless Commun. Control*, vol. 11, no. 5, pp. 505–517, Jun. 2021, doi: 10.2174/2210327910999201009163958.

[3] O. V. Bisikalo, V. V. Kovtun, and O. V. Kovtun, "Modeling of the estimation of the time to failure of the information system for critical use," in *Proc. 10th Int. Conf. Adv. Comput. Inf. Technol. (ACIT)*, Deggendorf, Germany, Sep. 2020, pp. 140–143, doi: 10.1109/ACIT49673.2020.9208883.

[4] S. Colabianchi, F. Costantino, G. Di Gravio, F. Nonino, and R. Patriarca, "Discussing resilience in the context of cyber physical systems," *Comput. Ind. Eng.*, vol. 160, Oct. 2021, Art. no. 107534, doi: 10.1016/j.cie.2021.107534.

[5] H. S. Lallie, K. Debattista, and J. Bal, "A review of attack graph and attack tree visual syntax in cyber security," *Comput. Sci. Rev.*, vol. 35, Feb. 2020, Art. no. 100219, doi: 10.1016/j.cosrev.2019.100219.

[6] V. Kovtun, I. Izonin, and M. Gregus, "Formalization of the metric of parameters for quality evaluation of the subject-system interaction session in the 5G-IoT ecosystem," *Alexandria Eng. J.*, vol. 61, no. 10, pp. 7941–7952, Oct. 2022, doi: 10.1016/j.aej.2022.01.054.

[7] P. G. George and V. R. Renjith, "Evolution of safety and security risk assessment methodologies towards the use of Bayesian networks in process industries," *Process Saf. Environ. Protection*, vol. 149, pp. 758–775, May 2021, doi: 10.1016/j.psep.2021.03.031.

[8] L. Zhang and V. L. L. Thing, "Three decades of deception techniques in active cyber defense–retrospect and outlook," *Comput. Secur.*, vol. 106, Jul. 2021, Art. no. 102288, doi: 10.1016/j.cose.2021.102288.

[9] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101677, doi: 10.1016/j.cose.2019.101677.

[10] S. I. Pérez, S. Moral-Rubio, and R. Criado, "A new approach to combine multiplex networks and time series attributes: Building intrusion detection systems (IDS) in cybersecurity," *Chaos, Solitons Fractals*, vol. 150, Sep. 2021, Art. no. 111143, doi: 10.1016/j.chaos.2021.111143.

[11] C. Senarak, "Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel," *Asian J. Shipping Logistics*, vol. 37, no. 4, pp. 345–360, Dec. 2021, doi: 10.1016/j.ajsl.2021.10.002.

[12] Ž. Turk, B. G. de Soto, B. R. K. Mantha, A. Maciel, and A. Georgescu, "A systemic framework for addressing cybersecurity in construction," *Autom. Construct.*, vol. 133, Jan. 2022, Art. no. 103988, doi: 10.1016/j.autcon.2021.103988.
[13] R. van der Kleij, J. M. Schraagen, B. Cadet, and H. Young, "Developing decision support for cybersecurity threat and incident managers," *Comput. Secur.*, vol. 113, Feb. 2022, Art. no. 102535, doi: 10.1016/j.cose.2021.102535.
[14] G. Delaval, A. Hore, S. Mocanu, L. Müller, and É. Rutten, "Discrete control of response for cybersecurity in industrial control," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 1747–1754, 2020, doi: 10.1016/j.ifacol.2020.12.2295.
[15] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," *Comput. Secur.*, vol. 102, Mar. 2021, Art. no. 102154, doi: 10.1016/j.cose.2020.102154.
[16] K.-F. Cheung, M. G. H. Bell, and J. Bhattacharjya, "Cybersecurity in logistics and supply chain management: An overview and future research directions," *Transp. Res. E, Logistics Transp. Rev.*, vol. 146, Feb. 2021, Art. no. 102217, doi: 10.1016/j.tre.2020.102217.
[17] Y. Jiang and Y. Atif, "A selective ensemble model for cognitive cybersecurity analysis," *J. Netw. Comput. Appl.*, vol. 193, Nov. 2021, Art. no. 103210, doi: 10.1016/j.jnca.2021.103210.
[18] A. Ray, "Cybersecurity risk management-I," in *Cybersecurity for Connected Medical Devices*. Amsterdam, The Netherlands: Elsevier, 2022, pp. 137–183, doi: 10.1016/B978-0-12-818262-8.00005-X.
[19] A. Ray, "The product cybersecurity organization," in *Cybersecurity for Connected Medical Devices*. Amsterdam, The Netherlands: Elsevier, 2022, pp. 117–136, doi: 10.1016/B978-0-12-818262-8.00011-5.
[20] Y. Hong and S. Furnell, "Understanding cybersecurity behavioral habits: Insights from situational support," *J. Inf. Secur. Appl.*, vol. 57, Mar. 2021, Art. no. 102710, doi: 10.1016/j.jisa.2020.102710.
[21] O. Ogbanufe, D. J. Kim, and M. C. Jones, "Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures," *Inf. Manage.*, vol. 58, no. 7, Nov. 2021, Art. no. 103507, doi: 10.1016/j.im.2021.103507.
[22] X. Yuan, S. Liu, M. A. Valdebenito, M. G. R. Faes, D. J. Jerez, H. A. Jensen, and M. Beer, "Decoupled reliability-based optimization using Markov chain Monte Carlo in augmented space," *Adv. Eng. Softw.*, vols. 157–158, Jul. 2021, Art. no. 103020, doi: 10.1016/j.advengsoft.2021.103020.
[23] Q. Zhang and Y. Liu, "Reliability evaluation of Markov cyber–physical system oriented to cognition of equipment operating status," *Comput. Commun.*, vol. 181, pp. 80–89, Jan. 2022, doi: 10.1016/j.comcom.2021.10.004.
[24] B. Wu and L. Cui, "Reliability of multi-state systems under Markov renewal shock models with multiple failure levels," *Comput. Ind. Eng.*, vol. 145, Jul. 2020, Art. no. 106509, doi: 10.1016/j.cie.2020.106509.
[25] D. G. Savakar and A. Kannur, "Hidden Markov model for identification of different marks on human body in forensic perspective," *Int. J. Modern Educ. Comput. Sci.*, vol. 11, no. 3, pp. 38–45, Mar. 2019, doi: 10.5815/ijmecs.2019.03.06.
[26] H. Dalkani, M. Mojarad, and H. Arfaeinia, "Modelling electricity consumption forecasting using the Markov process and hybrid features selection," *Int. J. Intell. Syst. Appl.*, vol. 13, no. 5, pp. 14–23, Oct. 2021, doi: 10.5815/ijisa.2021.05.02.
[27] L. Y. Zhilyakova, "Graph dynamic threshold model resource network: Key features," *Int. J. Math. Sci. Comput.*, vol. 3, no. 3, pp. 28–38, Jul. 2017, doi: 10.5815/ijmsc.2017.03.03.
[28] A. Lazaridis and I. Mporas, "Evaluation of hidden semi-Markov models training methods for Greek emotional text-to-speech synthesis," *Int. J. Inf. Technol. Comput. Sci.*, vol. 5, no. 4, pp. 23–29, Mar. 2013, doi: 10.5815/ijitcs.2013.04.03.
[29] P. Dixit and S. Silakari, "Deep learning algorithms for cybersecurity applications: A technological and status review," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100317, doi: 10.1016/j.cosrev.2020.100317.
[30] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, vol. 347, pp. 149–176, Jun. 2019, doi: 10.1016/j.neucom.2019.02.056.
[31] L. J. Rashad and F. A. Hassan, "Artificial neural estimator and controller for field oriented control of three-phase I.M.," *Int. J. Intell. Syst. Appl.*, vol. 11, no. 6, pp. 40–48, Jun. 2019, doi: 10.5815/ijisa.2019.06.04.
[32] I. Izonin, N. Kryvinska, R. Tkachenko, K. Zub, and P. Vitynskyi, "An extended-input GRNN and its application," *Proc. Comput. Sci.*, vol. 160, pp. 578–583, Jan. 2019, doi: 10.1016/j.procs.2019.11.044.
[33] B. K. Tripathy and U. Bhambhani, "Properties of multigranular rough sets on fuzzy approximation spaces and their application to rainfall prediction," *Int. J. Intell. Syst. Appl.*, vol. 10, no. 11, pp. 76–90, Nov. 2018, doi: 10.5815/ijisa.2018.11.08.
[34] Z. Ullah, M. Fayaz, and S.-H. Lee, "An efficient technique for optimality measurement of approximation algorithms," *Int. J. Mod. Educ. Comput. Sci.*, vol. 11, no. 11, pp. 13–21, Nov. 2019, doi: 10.5815/ijmecs.2019.11.03.
[35] I. Tsmots, V. Teslyuk, and I. Vavruk, "Hardware and software tools for motion control of mobile robotic system," in *Proc. 12th Int. Conf. Exper. Designing Appl. CAD Syst. Microelectron. (CADSM)*, Feb. 2013, p. 368.
[36] J. Burkhardt, "Bayesian parameter inference of explosive yields using Markov chain Monte Carlo techniques," *Int. J. Math. Sci. Comput.*, vol. 6, no. 2, pp. 1–17, Apr. 2020, doi: 10.5815/ijmsc.2020.02.01.
[37] P. K. H. Kaluarachchilage, C. Attanayake, S. Rajasooriya, and C. P. Tsokos, "An analytical approach to assess and compare the vulnerability risk of operating systems," *Int. J. Comput. Netw. Inf. Secur.*, vol. 12, no. 2, pp. 1–10, Apr. 2020, doi: 10.5815/ijcnis.2020.02.01.
[38] I. El Korbi and L. A. Saïdane, "Performance evaluation of unslotted CSMA/CA for wireless sensor networks: Energy consumption analysis and cross layer routing," *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 6, pp. 1–12, Jun. 2017, doi: 10.5815/ijcnis.2017.06.01.

**VIACHESLAV KOVTUN** received the Ph.D. degree in information and measuring systems, in 2006, and the Dr.Sc. degree in information technologies, in 2021. He is currently a Professor at the Department of Computer Control Systems, Vinnytsia National Technical University, Ukraine. His main research interests include system analysis, information technologies, mathematical modeling, machine learning, pattern recognition, and signal processing.

**IVAN IZONIN** (Member, IEEE) received the M.Sc. degree in computer science, in 2011, the M.Sc. degree in economic cybernetics, in 2012, and the Ph.D. degree in artificial intelligence, in 2016. He is currently an Associate Professor at the Department of Artificial Intelligence, Lviv Polytechnic National University, Ukraine. His main research interests include computational intelligence, high-speed neural-like systems, non-iterative machine learning algorithms, and ensemble learning.

**MICHAL GREGUŠ** received the Ph.D. degree *(summa cum laude)* in mathematical analysis from the Faculty of Mathematics and Physics, Comenius University in Bratislava.

He has been working previously in the field of functional analysis and its applications. His research interests include management information systems, in modeling of economic processes and in business analytics.