Захист інформації та кібернетична безпека

UDC 681.32:007.5 DOI: 10.30748/soi.2019.159.08

O. Milov[1], L. Parkhuts[2], S. Milevskyi[1], S. Pohasii[1]

[1] *S. Kuznets Kharkiv National University of Economics, Kharkiv*
[2] *Lviv Politechnic National University, Lviv*

VERIFICATION OF THE SECURITY SYSTEMS ANTAGONISTIC AGENTS BEHAVIOR MODEL

Model verification is a very important step in the methodology for modeling the security systems antagonistic agents behavior in general and system dynamics in particular. By verifying the behavior model of antagonistic agents we mean a process that includes both formal/quantitative tools and informal/qualitative ones. The article presents the process of creating a model of antagonistic agents behavior. The assumptions underlying the model and the limitations of the created model are preliminarily formed. The components of the model are distinguished: a defender submodel, an attacker submodel and a confrontation environment submodel. For each of the submodels, the processes and relationships in models are described, the variables used for modeling are defined. Processes and relations between variables are presented in the form of a system of linear and differential equations. Based on the given system of equations of the mathematical model, a system-dynamic model of the interaction of antagonistic agents is constructed. It is shown that for the practical use of the software implementation of the behavior model, the verification procedure is mandatory. The main groups of tests that need to be performed using the model are listed to confirm its adequacy to the conditions of use and the goals for which it was developed. The results of testing the system-dynamic behavior model for the main group of verification tests at each of the three main stages of model verification are presented: structural tests, structure-oriented behavior tests and behavior model tests. Based on the results obtained, the special importance of structurally oriented behavioral tests is emphasized. These are powerful behavioral tests that can provide information about potential structural weaknesses. These tests seem to be the most promising area for research on model verification.

Keywords: *verification, behavior model, antagonistic agents, system-dynamic model, model adequacy.*

Introduction

The Internet revolution has dramatically changed the way people, firms and governments communicate and conduct business. But at the same time, this global interconnectedness increased the vulnerability of computer systems to information security breaches [1–2]. Protecting information systems, data, intellectual property and business processes from attacks, misuse or technical failures has become and is projected to remain a key challenge for organizations [3–7].

In efforts to protect data and systems, research conducted by practitioners and scientists focused mainly on the technical aspects of cybersecurity, that is, on the issues of which assets need to be protected at a certain level and which security countermeasures provide this protection. Given the high cost of cybersecurity measures and budgetary constraints, a "fully protected organization" is not only a complex, but also an unattainable goal [8]. Instead of total protection of the organization, it is necessary to consider the business processes of the organization, on which the financial well-being of the organization depends, which can be considered as the goal of the organization functioning. This view reflects a service-oriented approach that defines important services and service packages in an organization. Threats and vulnerabilities are evaluated in the context of services, and not for individual assets. Because an organization has fewer services than assets, analysis takes less time and is better managed than assets. A service-oriented perspective is better associated with generating business revenue [8].

The practice of cyber defense of business process circuits has demonstrated the following feature. The effectiveness of cyber defense of the business processes contours depends on the volume of investments that are sent in the relevant areas. In this case, decisions on the allocation of certain amounts fit into the "wait and see" scenario, i.e. decisions are reactive and are made upon the implementation of a successful cyber attack. On the other hand, the attacker acts according to the scenario of the "weakest link". Thus, the effectiveness of the creation and functioning of cyber defense systems is determined by the behavioral characteristics of the attacking

and defending sides, which can be considered as confirmation of the relevance of developing models of the behavior of the interacting parties to cyber conflict.

For practical use of the developed model of antagonistic agents behavior simulation results, it is necessary to be sure that the model correctly displays the real processes of security system agents interaction.

Therefore, checking the correctness of the model, its adequacy and compliance with the real processes in security systems is an urgent problem of creating and developing a system for protecting business processes from various kinds of cyber attacks.

The purpose and objectives of the study. The aim of the work is the development and subsequent verification of antagonistic agents behavior model under conditions of cyber conflict, the purpose of which is the possibility of scenario modeling of the parties to cyber conflict behavior. Verification of the developed model should ensure the reliable use of simulation results.

To achieve this goal it is necessary to solve the following tasks:

− identify the basic concepts used in the interaction models of antagonistic agents and directly affect the decision on the direction of investment to protect against a particular attack vector, as well as the assumptions and limitations of the model;

− to develop mathematical models for the interaction of parties to the conflict that affect the adoption or change of previously made investment decisions;

− to determine the verification procedure and the tests following from it, in order to verify the developed model;

− to verify the developed model by implementing simulation based on the developed mathematical model to confirm the logic of behavior of the parties to the conflict and assess the impact of their behavior on the use of investments.

Statement of basic materials

Development of a model of the behavior of antagonistic agents in security systems

When developing a model of behavior, it is first necessary to determine the boundary of applicability of the model and the main assumptions included in it. The proposed model focuses on the dynamics of the interaction of the attacker and the defender in the field of information security to determine the investment strategies used by opponents.

The model represents the company as a defender, which protects the asset from a group of attackers who are trying to violate the security of the company's asset with the help of malicious cyber attacks. An asset can take many forms, such as a customer list, website, payables register, or strategic plan. Increased security may be associated with protecting the confidentiality, integrity, authenticity or availability of the asset for authorized users.

Modeling is limited to three possible threat vectors. Protection against each of the threat vectors is realized as a result of investing in appropriate protection. Defense is considered effective if it can compensate for incoming attacks.

The list of basic concepts and concepts underlying the developed model, which underlie the interaction of the defender and the attacker in a dynamic behavior model, includes the following [9].

1. Reputation of the company – a profitable and universally recognized name for merits, achievements, reliability, etc. In this case, the reputation refers to the public authority of the company.
2. Vulnerability is the level of security possessed by company assets. It can also be called an asset protection level.
3. Security vectors are externally visible and accessible system resources that can be used to organize attacks on the system. The weight (or magnitude) of the vector is specified in accordance with the potential damage that could be caused by any exploitation of the vulnerability. Examples of security vectors are: network servers, web pages, email, mobile devices, system configuration, and others.
4. Opportunities of defenders – available resources of defenders, which are distributed between security vectors to increase the level of protection of assets.
5. Opportunities for intruders – part of the resources of intruders available to implement attacks on defender assets.
6. The share of investment – part of the opportunities aimed at protecting the assets of the company.
7. Percentage of attacks – the number of attacks that cybercriminals distribute between the security vectors of defenders according to previous successful attacks.
8. Successful attacks – attacks that can violate asset protection through security vectors.
9. Profit of defenders – monetary gain from improving the level of asset security, which in turn increases the reputation, thereby improving the financial performance of the company.
10. Welfare of the attackers – a monetary advantage from the violation of the assets of the defenders.

The formed concepts should be included in the mathematical model, since they reflect the nature of the interaction of the parties to the conflict and influence the distribution of limited investment funds.

To get an idea of the dynamics of the attacker-defender interactions, a quantitative and integrative dynamic model with a suitable border, time horizon and a realistic interpretation of strategic decisions by individuals is needed.

The model consists of three submodels: Defender Submodel, Battlefield Submodel and Attacker submodel.

The model was built on the following assumptions and limitations.

Assumption 1: The impact of cyberattacks on a firm's reputation.

There are both direct and indirect costs associated with cyber security breaches. Direct costs for companies include, for example, money spent on intrusion detection systems, overtime for hack recovery personnel, and, for example, lost productivity during virus attacks. However, these are the costs that companies face in the daily work of their business in the world of the Internet. The direct costs of cybersecurity are not included in the analyzed model.

The real financial damage from cyber security breaches is associated with indirect costs [10]. These can be losses caused by falling sales, weakening customer relationships and legal obligations. Indirect costs are difficult to measure, but they must be presented in the model, since they can significantly affect the company's income.

The company's reputation is fundamental. Loss of reputation is considered the indirect costs that the company incurs as a result of cyber attacks. An ad or an article containing a security breach may affect their reputation and financial performance. An example of this is a virus attack on bank ATMs, which causes them to close for several hours, this may bother customers, but they probably will not change banks in connection with this incident. However, if the bank is hacked and customer data is distributed on the Internet, customers may well decide to start their own business elsewhere. In the latter case, the violation had a negative impact on the reputation and, consequently, on the market value of the company due to the real potential for loss of future revenue when customers change the service bank [11].

The analyzed model assumes the value for each of the three security vectors as the weight coefficient that they attach to their reputation, as well as the status of vector vulnerabilities and successful attacks. Modeling will provide an understanding of the value that the company attaches to cybersecurity to maintain its reputation.

Assumption 2: The capabilities of defenders and attackers are external parameters.

A firm's ability to invest in information security is limited by its finances. In particular, information security should compete with other projects for financing [12]. Given budgetary constraints, the more difficult task for managing information security is not so much the general level of the required level of investment as the allocation of limited resources to protect against attacks [13].

Depending on the size of the company and the industry to which it belongs, the capabilities of firms will vary. The model assumes a relatively large company, since the budget for information security does not depend on the financial performance of the company. In other words, the budget for investing in information security in this case is fixed and affordable for each modeling period.

Opportunities for attackers are also assumed to be constant for each period. In a real system, hackers are criminal organizations that act in accordance with their own business model. Therefore, it is not known exactly how the attackers behave, and on what they build their business case and, therefore, how they form their resources for future attacks. The model reflects the behavior and capabilities of attackers described in the literature.

Assumption 3: The cost of a single attack. The cost of a single attack means the ratio of the capabilities of attackers and defenders. This parameter represents the damage that each attack does to the defenders. In other words, the cost of a single attack is how much money a defender needs to repel an attack.

In the model, the cost of a single attack is an exogenous variable. This option will increase the ability of attackers to determine the vulnerability status of each security vector.

Assumption 4: Type of attackers and type of attacks. Cyber attacks can come from inside or outside the company. The model makes no distinction between internal and external attackers. Internal attackers include disgruntled and / or negligent employees who use a weak password to access the system or follow a link from a phishing site, not knowing that it is malicious software. Another type of attacker is an external one, generally including hacker organizations of criminals. In addition, the model does not break attacks into various types, for example, denial of service, phishing, viruses, ransomware, SQL injections, and so on.

Assumption 5: The cost of security for defenders. In the model, the cost of security that defenders bear when making an investment decision each period is reflected in the decision rule on the share of investments that they allocate for each security vector when it is violated.

The model does not reflect various financial indicators and does not use approaches to analyze each investment decision, such as: cost-benefit analysis, risk analysis, net present value (NPV), annual loss estimation (ALE), return on securities investment (ROSI) etc. The reason for this is that financial analysis would require a more complex model, including empirical data, to give greater accuracy to research.

The structure of the model represents both a qualitative display of the system, through causal relationships between variables, and its quantitative representation, by formally determining causal relationships through equations.

The system dynamics model contains three submodels:

- Defender Submodel;

- Battlefield Submodel;
- Attacker Submodel.

The Defender Submodel represents the structure of a firm's defense against malicious cyber attacks that attempt to violate the security of its information asset. In each period, the defender makes a decision to determine his defense configuration. It is assumed that defenders have basic protection for each vector, and their security capabilities are designed to cover the additional security efforts resulting from security breaches.

We introduce the following notation for the variables and factors describing the Defender Submodel (Tabl. 1).

Table 1

Formal designation used in Defender Submodels

A_i^{RS}	*Reported Successful Attacks*$_i$
A_i^{S}	*Successful Attacks*
T^{RA}	*Time to report Attack*
N^{DA}	*Number of Dismissed Attacks*
T^{D}	*Dismissal time*
D	*Dismissed*
R	*Reports*
FI_i	*Fraction Investment Vector i*
Rep	*Reputation*
BU	*Building Up*
T^{BUR}	*Time to build up reputation*
Adj	*Adjustment/*
ER	*Erosion*
T^{RL}	*Time reputation loss*
R^{B}	*Base reputation*
V_i	*Vector i Value*
Vul_i	*Vulnerability Vector i*
DFP	*Defenders Financial Performance*
RMR	*Reputation to money rate*
BFP	*Base financial performance*
DAP	*Defenders Accumulated Profit*
IFP	*Increasing Financial Performance*

Defender protects his asset against three security vectors (A, B and C) that matter, which will be converted into reputation and then into financial results. In the model, security vectors are presented as the vulnerability state of each vector.

In case of successful attacks, a message is generated indicating the specific attack vector by which the target of the attack was achieved.

A description of the dynamics of successful attacks for each of the vector can be represented in the form of the following relationships:

$$\frac{d\left(A_i^{RS}\right)}{dt} = R_i - D_i;$$

$$R_i = A_i^{S} / T^{RA},$$

where R_i– increase in the number of successful attacks on a specific vector during the time required by the defender to report successful attacks (1 month);

D_i − the number of reflected attacks reported, divided by the time required by the defenders to stop such attacks (1 month).

The share of the investment vector for each vector is calculated based on the reported successful attacks divided by the sum of the recorded successful attacks of all three vectors. The equation indicates that the defender will invest a share of investments in the *i*-th vector, which is equal to the total number of successful attacks received on this vector

$$FI_i = A_i^{RS} / \sum_{i=1}^{3} A_i^{RS}.$$

Reputation is presented as a stock that accumulates during each modeling period. Reputation enhancement is the growth rate obtained by adjusting the reputation, which, in turn, is the result of the sum of the values of each security vector and their corresponding vulnerability result for each vector.

$$\frac{d\left(Rep\right)}{dt} = BU - ER;$$

$$BU = \begin{cases} Ad / T^{BUR} \ if \ \ Ad > 0; \\ 0 \ if \ \ Ad \le 0; \end{cases}$$

$$ER = \begin{cases} \left| Ad / T^{RL} \right| if \ \ Ad < 0; \\ 0 \ if \ \ Ad \ge 0. \end{cases}$$

Raising a reputation is the following decision-making rule: reputation growth rate will increase whenever the adjustment is positive. On the contrary, a negative adjustment (loss of reputation) means that the company is losing its reputation.

$$Ad=IR–Rep;$$

$$IR = R^{B} - \sum_{i=1}^{3} V_i \times Vul_i.$$

Financial Performance of Defenders. Financial indicators of defenders are determined by the current reputation and the ratio of the level of reputation to funds, which shows how much the reputation of the company is estimated in relation to its financial indicators:

$$DFP=(RMR*Rep)+BFP.$$

Defenders Profit determined by financial indicators, which is necessary for the analysis of policy options.

$$\frac{d\left(DAP\right)}{dt} = IFP.$$

The Battlefield sub-model is a segment of the model in which defenders and attackers interact with their respective capabilities and investment decisions. The main components of this submodel are Vulnerability and Successful attacks of each security vector.

In the description of the submodel of the battlefield, the following notation of variables is used (Tabl. 2).

Table 2

Description of Variable Submodels of the Battlefield

C^A	Attackers Capabilities
AF_i	Fraction of Attack Vector *i*
C^{UA}	Attack Unitary Cost
C^D	Defenders Capabilities

Vulnerability of attack vectors indicates the level of security for each of the vectors. If the vulnerability is positive, it means that the system is weak in security. Vulnerability is determined by the following expression:

$$Vul_i = \left(C^A \times AF_i \times C^{UA}\right) - \left(C^D \times FI_i\right).$$

In essence, the vulnerability is determined by the difference between the resources that the attacker directs to the corresponding vector of attacks and the resources that the defender allocates to fix security flaws on the same vector. The resources of an attacker are determined by his abilities, multiplied by the fraction of the capabilities allocated for attacking the vector, and by money, for the attack equivalent to each attack. Similarly, the resources of the defender are the result of the multiplication of his abilities and the share intended to protect the vector after hacking.

Successful attacks are important for this model, as they will trigger future investment decisions for both opponents. Successful attacks are calculated as follows:

$$SA_i = \begin{cases} \left(C^A * AF_i\right) - \left(\left(C^D * AF_i\right) / C^{UA}\right) \; if \; Vul_i > 0; \\ 0 \;\; if \; Vul_i \le 0. \end{cases}$$

This formulation entails that if the vulnerability of the vector is below zero, there will be no successful attacks, since the defender has equal or superior capabilities than the attacker, and he is able to stop all attacks. On the other hand, if the vulnerability of a vector is above zero, there will be successful attacks.

Multiplying the defender's capabilities by the share of invested funds, and then divided by the cost of a single attack, indicates the number of attacks that the defender can reflect in case of a security violation. Thus, the difference between the number of attacks carried out for each vector and the number of attacks that the defender can repel is equal to the total number of successful attacks.

The attacker is aimed at the company and makes some efforts to implement attacks. Since the attacker does not know where to aim in order to gain profit, he uses the initial distribution of successful attacks to determine the distribution of vulnerabilities by vectors.

The attacker identifies and uses the weakest link, i.e. the security vector with the lowest protection. If the attacker succeeds, he will make a profit, which will mean lower financial performance for the defender. The attacker does not act indiscriminately; rather, he attacks only when it is beneficial to him.

Successful historical attacks in the attacker's model prompt to attack the weakest link and not neglect other vectors, allocating a smaller part of the resources for their attack. It is assumed that the attacker obtains the same utility for using all security vectors.

To represent the relations that determine the attacker's behavior, the following notation of variables has been introduced (Tabl. 3).

Table 3

Variable designations for an attacker submodel

A_i^{AS}	Accumulated Successful Attacks Vector *i*
B	Breaches
A_i^S	Successful Attacks Vector *i*
T^{RA}	Time to report attack
V_i^P	Past value *i*
S_i	Switch *i*
P^A	Attackers Performance
B_i	Breaches Vector *i*
W^{AA}	Accumulated Attackers Wealth
W^{IA}	Increasing Attackers Wealth

Accumulated successful attacks. The sum of the accumulated successful attacks of each vector allows the attacker to determine the weakest link and determine the solutions for the next attack in order to use the most vulnerable security vector. The designation *i* indicates the vectors *A*, *B* and *C*.

$$\frac{d\left(A_i^{AS}\right)}{dt} = B_i;$$

$$B_i = A_i^S / T^{RA}.$$

The increase in this indicator is determined by successful attacks in the vector, divided by the time it takes for attackers to report attacks (1 month).

Share of attack vectors-are decisions made by attackers as a result of accumulated successful attacks on each vector. For the weakest link strategy to work in this model, attackers must switch from one vector to another when the current vector is not good enough for him to continue to attack him.

For this reason, the parameter of the past value is used to save the previous value of the previous period in order to be able to compare the current value of the at-

tack with the past value of the accumulated successful attacks for the last period and determine whether it increases or decreases in order to decide whether or not to change the vectors.

$$V_i^P(t) = A_i^{AS}(t-1);$$

$$S_i = \begin{cases} 0 \; if \; A_i^{AS} - V_i^P < 1; \\ 1 \; if \; A_i^{AS} - V_i^P \geq 1. \end{cases}$$

Switch parameter is a condition that indicates that when the comparison of the current value with the previous value is less than 1, then the switch becomes zero, and it is not advantageous for the attacker to continue using this vector and move on to another. The conditional value is 1, not zero, since 1 is a threshold for evaluating the differences between the two values, which must be at least equal to one to justify the change.

This is an example of calculating the attack fraction of the vector A, but for the other vectors the same:

$$A_i^F = S_i \times A_i^{AS} / \sum_{i=1}^{3} S_i \times A_i^{AS} .$$

Whenever an attacker decides to stop attacking one vector and switch to another, investments in the other two vectors will increase.

Attacker performance– this is the sum of violations of all vectors multiplied by the cost of a single attack:

$$P^A = \sum_{i=1}^{B} B_i \times C^{UA} .$$

The "welfare" of attackers is determined by financial indicators; this stock was created for analysis purposes in the following scenario and policy options analysis. The influx of wealth of attackers is a function of the productivity of attackers.

$$\frac{d(AAW)}{dt} = IAW .$$

Verification of the system-dynamic model

In any simulation-based study, you need to know how much you can trust model-based analysis. The process of system-dynamic modeling is iterative, in which various tests are used to carefully study the model and to be sure of its usefulness. Such a process allows us to understand the relationship between the structure of the system and its behavior. Formal processes that lead people to confidence in a model are often called model validation. There is little agreement between the various modeling methodologies about what good evidence is or what it should be. A review of the literature shows that, in fact, there is no general suitable procedure for verification that a system-dynamic model must pass in order to be considered valid [14–15].

An iterative approach to formulating a model is usually due to the complexity of the problem being solved. However, despite numerous iterations during the modeling process, no model has ever been or never will be fully tested (Greenberger et al., 1976), mainly because all of them are simplified representations of reality.

In [14], it was noted that validity in system dynamics refers to the internal structure of the model, and not to the output behavior. Behavioral replication alone is not enough to accept validity, as you can get "right behavior for the wrong reason". Instead, models have a specific goal, with which they can be verified, then the verification process should be aimed at achieving the goal of the model.

Despite the limitations of verification, limiting its qualitative and iterative nature, a logical sequence was proposed in [14] as a guide for conducting model validity tests in three stages: direct structural tests, structure-oriented tests, and behavior prediction. Any of these tests alone, of course, is not suitable as an indicator of the reliability of the model. But used together, they are a tough filter that can capture and filter out weaker models and allow the use of those that are most likely to reflect something close to the truth.

Structural validity.

Direct structural tests evaluate the reliability of the structure of a model by direct comparison with knowledge of the real structure of the system. This means comparing each equation and the logical function of the model separately with the existing knowledge relations about the real system. In such tests, imitation is not involved. The following tests belong to the category of structure tests, which include comparing the structure of a model with generalized knowledge of a system existing in the literature, taking into account the purpose of this model.

The purpose of the structure validation test is to compare the model equations with the relationships that exist in a real system, in this case the conceptual basis of the model is based on a systematic review of the information security literature during the model building process. An example of the confirmation of the structure performed during the modeling process relates to the structure of how the security level of each security vector and potential losses from such a security vector affect the investment strategy of the future distribution of opportunities among access vectors in order to protect the company's information asset.

The most common strategy used by a defender to allocate information security costs is the wait and see approach. Due to the uncertainties associated with potential information security breaches, security managers may find it economically rational to take a wait and see attitude regarding the use of available security features until a breach occurs. When the attack succeeds with the security vector, the defense constantly reports such attacks in order to be able to substantiate its next decision regarding the share of investments, which will be addressed to the vector that is violated most often.

According to the literature on real conditions [16–18], the expectation of key events often gives higher expected benefits from investments than if you act as if the investments were made at the moment or not done at all.

The literature shows that before investing, the net present value (NPV) of today's investment should be greater than the option cost associated with deferring the decision until more information appears.

Parameter Confirmation Test ensures that the values of all parameters are reasonable, and each variable and constant has a clear meaning in real life. The parameter estimate is constantly confirmed on the basis of the knowledge available in the literature, both conceptually and numerically.

Conceptual confirmation was carried out by determining the elements available in the literature that correspond to the model parameters. Numerical confirmation was carried out by evaluating the numerical value of the parameter with sufficient accuracy and probable ranges.

Some technical parameters are created for modeling purposes only, although real data may not be available. For example, some technical parameters, such as the capabilities and cost of a single attack, were evaluated to illustrate the dynamics of the defender and attacker investment strategies.

Studying the meaning of all parameters in a model helps to obtain a more accurate and reliable understanding of the model and to find that the aggregated structure is acceptable for research purposes.

Extreme direct test confirms that each solution (model equations) leads to a plausible conclusion at extreme values. The test was carried out by assessing the likelihood of the obtained values in comparison with the knowledge/expectation of what will happen under similar conditions in a real system.

For each flow equation in the model, extreme conditions were specified. For example, the maximum and minimum values were entered into the input variables and the values of the output variable were compared with what would logically occur in a real system under the same extreme conditions.

As an example of this test, the Violations for Attackers and Reported Attacks for Defenders flows were tested. These flows represent attacks that have been successful and encourage attackers to identify and use the weakest links, while defenders also identify the weakest links and protect their assets.

Assuming that if the capabilities of the defenders increase sharply compared to the capabilities of the attackers, there will be no successful attacks, and the defender will benefit. Meanwhile, if the capabilities of the attackers far exceed the capabilities of the defenders, successful attacks will significantly increase the damage done to the defenders and enhance the strengths of the attackers.

Dimension Matching Test. The system dynamics model has a dimension for each of its variables. The dimension for each variable is indicated when constructing the model, the consistency test of dimensions does not reflect anything but the error of the unit of measurement or missing units. Dimension consistency checking is usually automatically performed by the system dynamics software used for this study (Powersim Studio 9), which does not allow the use of the model without coordinating the dimensions of all equations. This test helps to evaluate whether the units of measure on the left and right sides of each equation coincide, without using any arbitrary “scaling” parameters that do not make sense in the real world [14–15]. A model is considered dimensionally consistent if it does not generate separate error messages when starting the simulation process.

Structurally-oriented behavior tests indirectly evaluate the validity of the structure by applying a specific test of behavior to the models of behavior generated by the model. These tests include simulation and are considered strong behavioral tests that can help the model designer identify potential structural flaws.

Test for extreme condition simplies assigning extreme values to certain parameters and comparing the simulated behavior of the observed or expected behavior of a real system under the same conditions.

A good example of an extreme test is the ability of defenders and attackers. These parameters are exogenous in the model and play an important role in determining the security level of each access vector to the information asset that the company is trying to protect.

For example, higher opportunities for either of the two adversaries will mean an increase or decrease in the security level of each vector, which, therefore, will translate into more or less successful attacks that trigger investment strategies for future periods.

An extreme conditions test, including the capabilities of defenders, can help verify that the mechanism described is consistent with the correct mathematical formulation. This is especially important because if firms set aside a higher budget for security measures, this would mean more protection and fewer successful violations of the firm's assets. A sudden change in this setting is unrealistic, as companies often have a relatively fixed budget for security measures. On the other hand, the possibilities of attackers can be drastically reduced, however, cybercriminals are IT professionals who are methodical in their actions. This means that they have a certain level of capabilities that they can plan to launch their business model.

Figure 1 shows the model’s response to extreme conditions for defenders. During the simulation experiment, the capabilities of the Defenders were changed to 10,000 euros, while the capabilities of the attackers remained the same. Since defenders can protect their as-

sets across all attack vectors, their financial performance increases because they maintain their reputation as high, and attackers cannot crack any of the vectors, and their state is zero (Fig. 2).

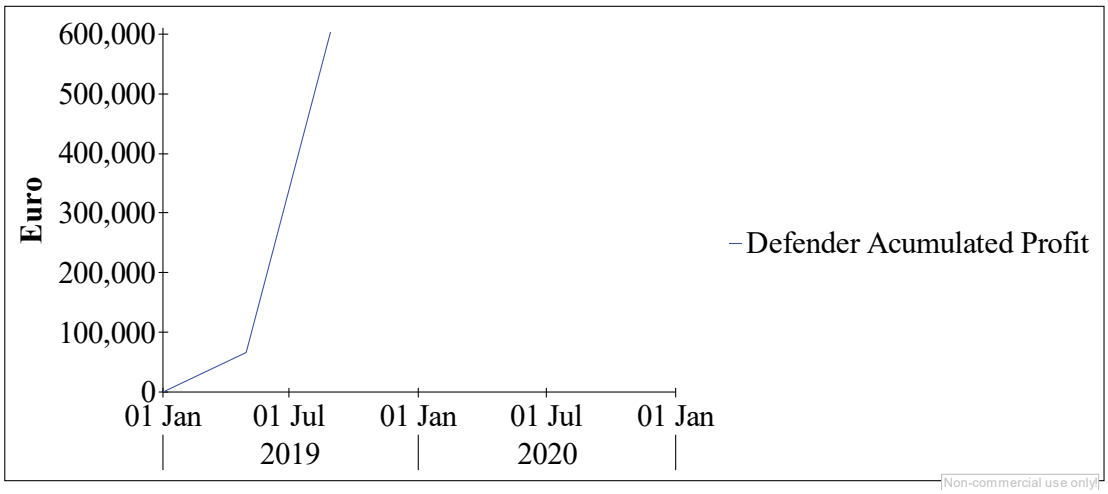

Fig. 1. Extreme test. The accumulated profit of the defenders with the dominance of their capabilities

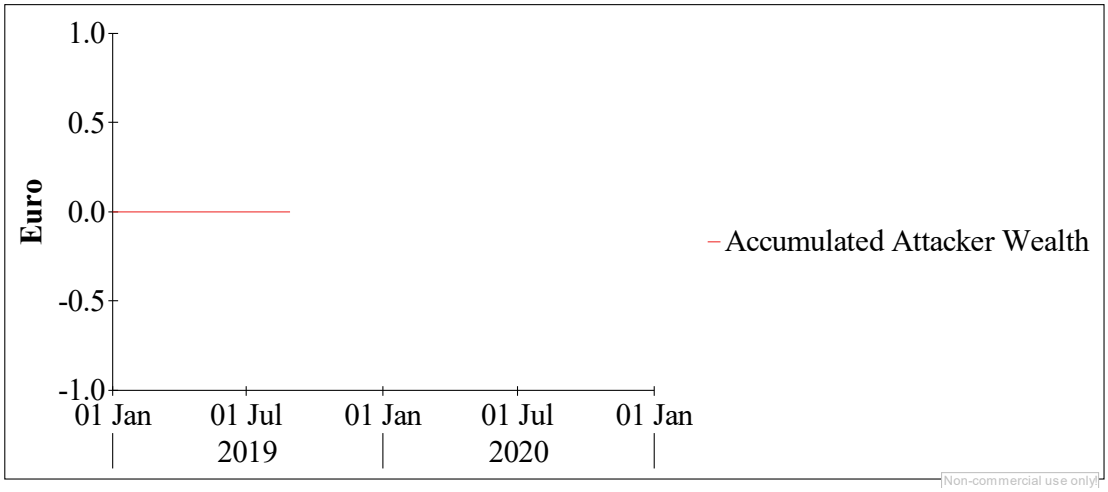

Fig. 2. Extreme test. The accumulated profit of attackers with the dominance of the capabilities of defenders

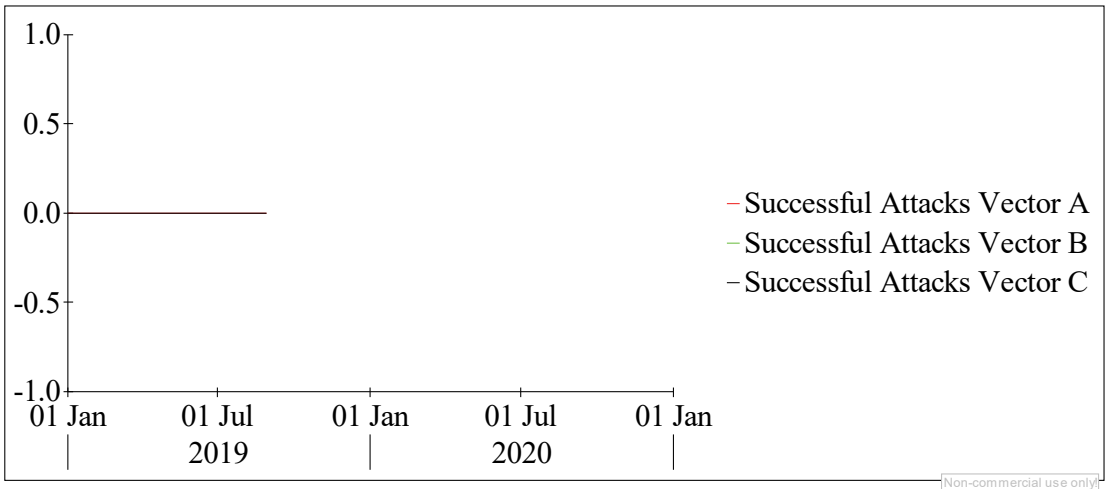

Fig. 3. Extreme test. Vectors of successful attacks with defenders' domination

Under these conditions, the vectors of successful attacks will remain at level zero, i.e. successful attacks will be absent (Fig. 3). And the vulnerability of the protection vectors will become negative, which corresponds to the case when not a single successful attack is implemented on a single security vector (Fig. 4).

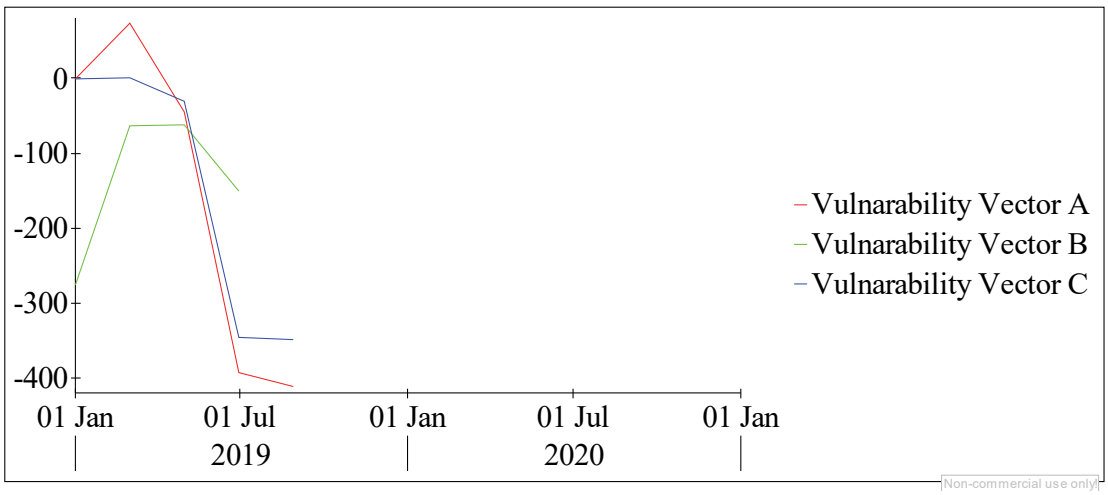

Fig. 4. Extreme test. Vulnerability of Protection Vectors

In Fig. 5 and Fig. Figure 6 shows the reaction of the model to extreme conditions for the capabilities of attackers. The attacker's capabilities were increased, and the defenders' capabilities remained the same. Since defenders cannot protect their assets in any of their vectors, their financial performance drops sharply because their reputation is very low, so attackers can violate all the defender's security vectors, and the welfare of attackers is growing.

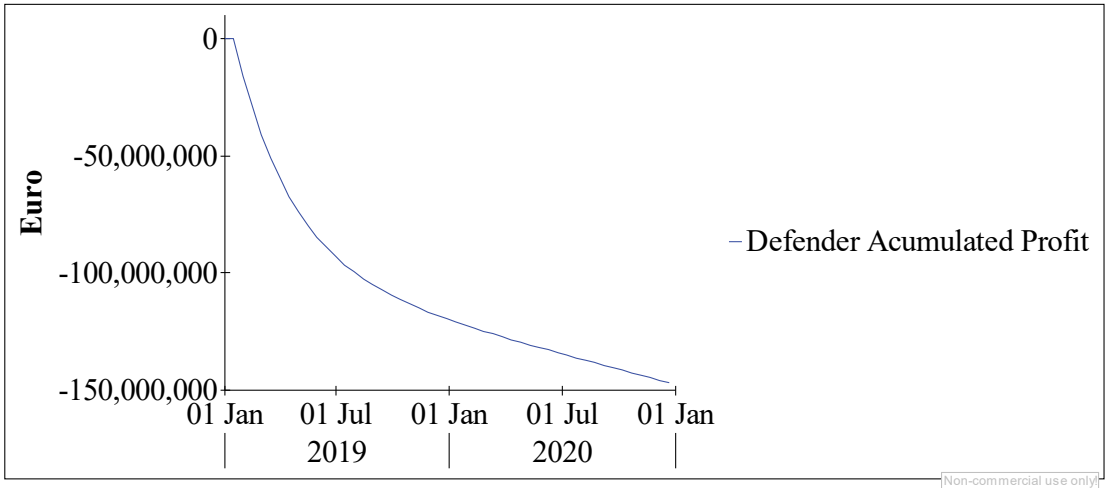

Fig. 5. The accumulated profit of defenders in the case of attackers' dominance

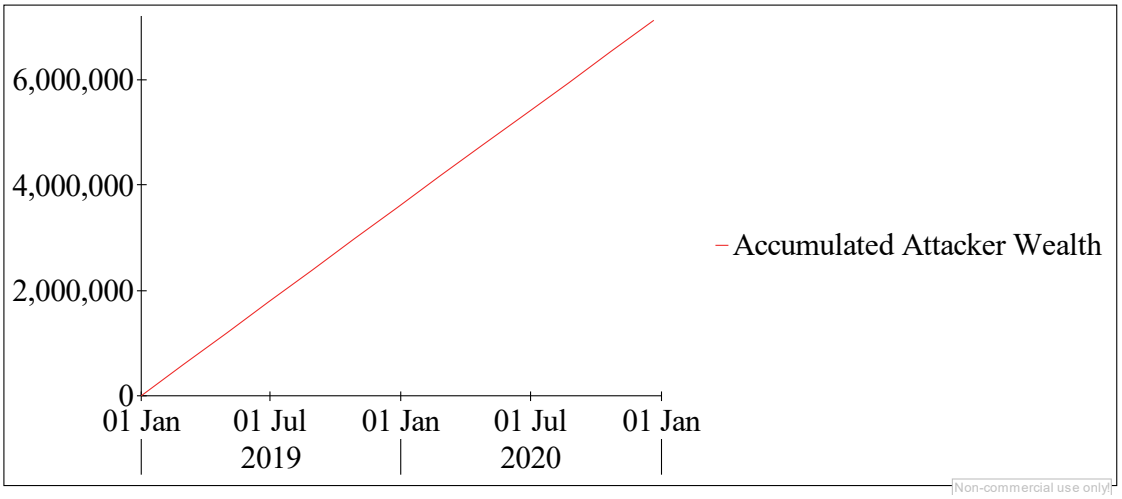

Fig. 6. The accumulated welfare of attackers when they dominate

Fig. 7 and Fig. 8 demonstrates the success of attacks on all vectors and the vulnerability of the corresponding vectors.

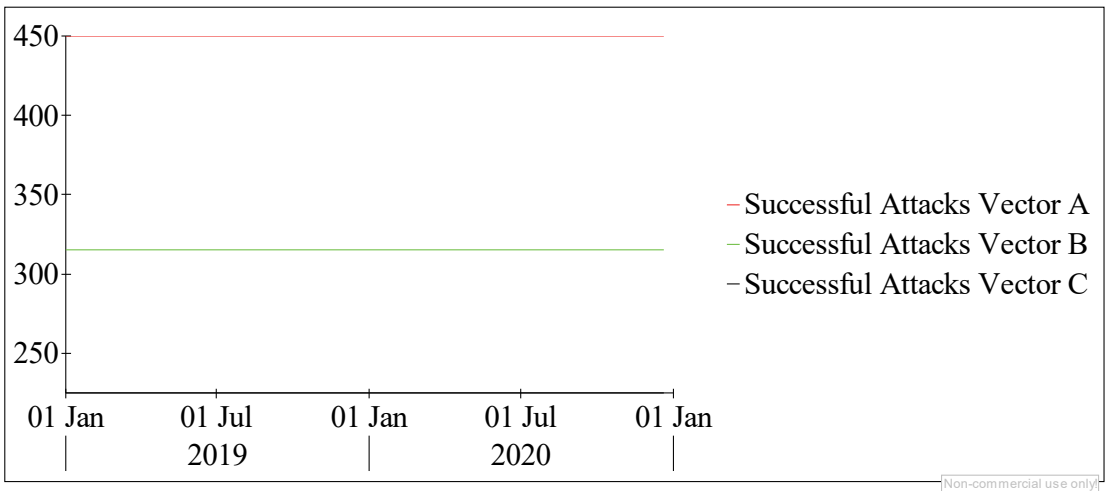

Fig. 7. The success of vector attacks with dominance of attackers

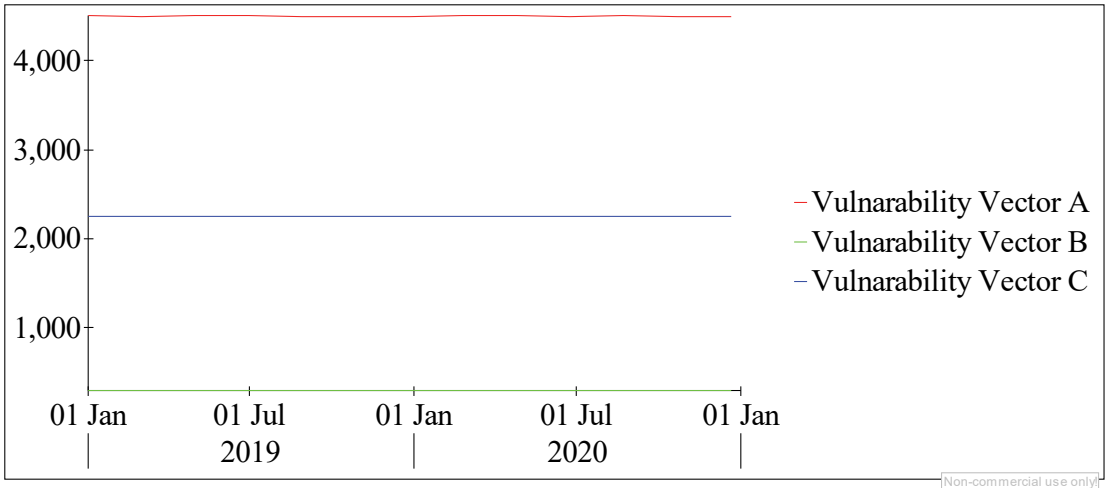

Fig. 8. Vulnerability of security vectors when attackers dominate

Behavior Sensitivity Test consists of determining those parameters to which the model is very sensitive, and figuring out whether the real system will exhibit such high sensitivity to the corresponding parameters. The following simulation presents the sensitivity analysis performed first, in the initial conditions of the model for accumulated successful attacks for vectors A, B and *C* (*A* = 5, *B* = 5, *C* = 10). Then a sensitivity analysis was carried out with changes in the unit cost of the attack (damage) (Fig. 9–13).

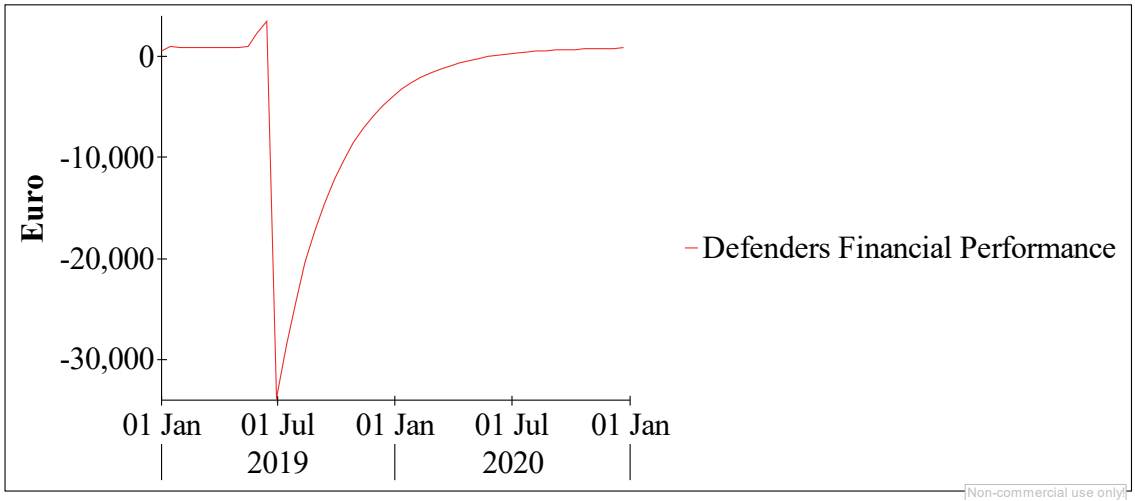

Fig. 9. Financial performance of defenders

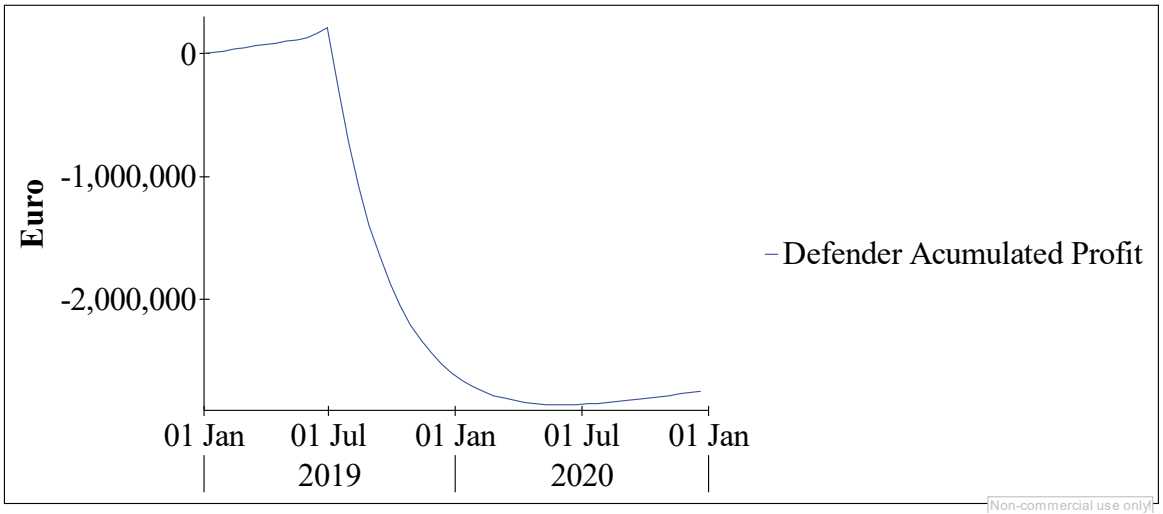

Fig. 10. The accumulated profit of the defenders

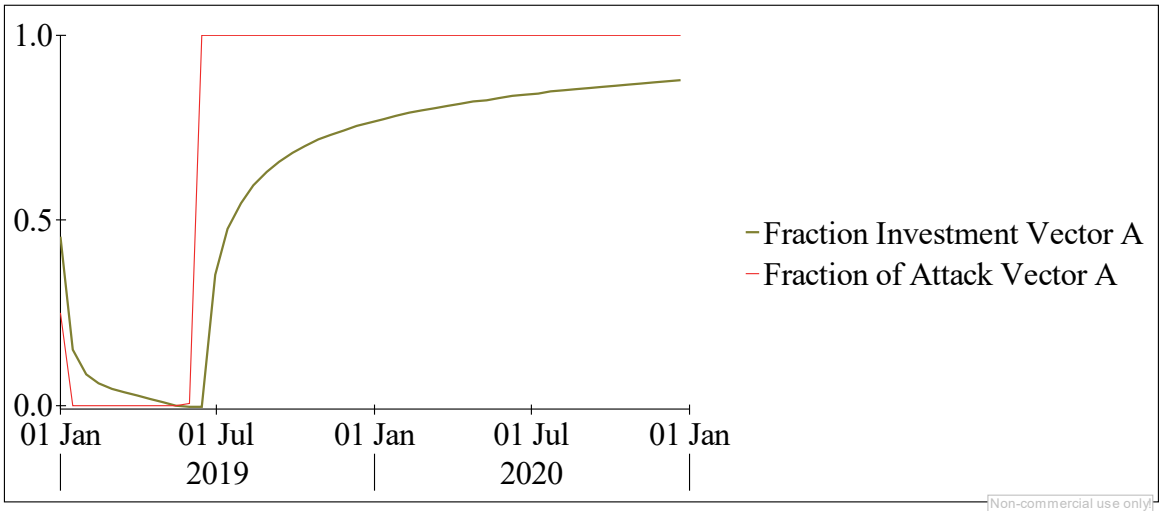

Fig. 11. The share of investments and the share of attacks on vector *A*

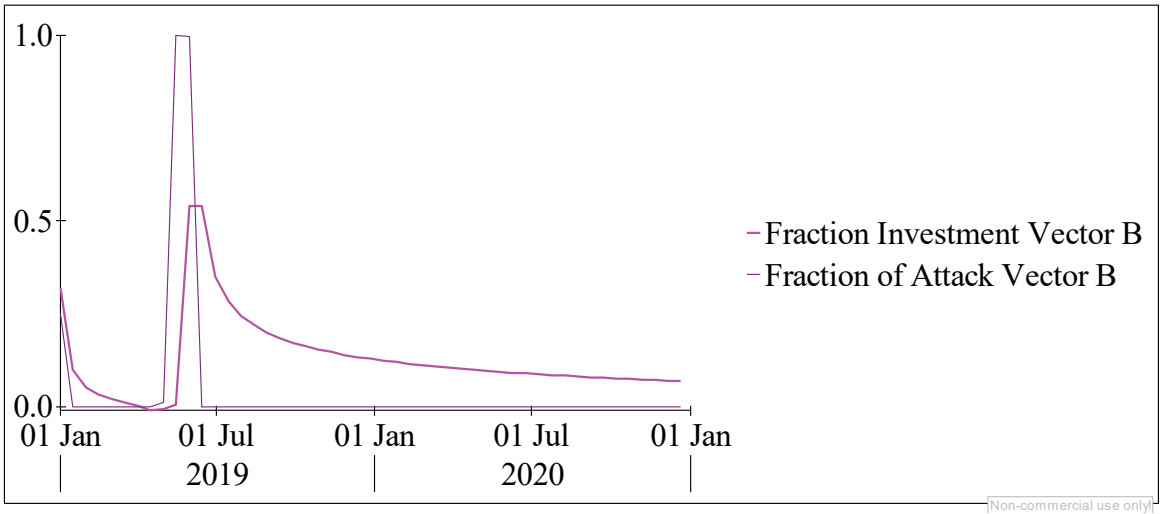

Fig. 12. The share of investments and the share of attacks on vector *B*

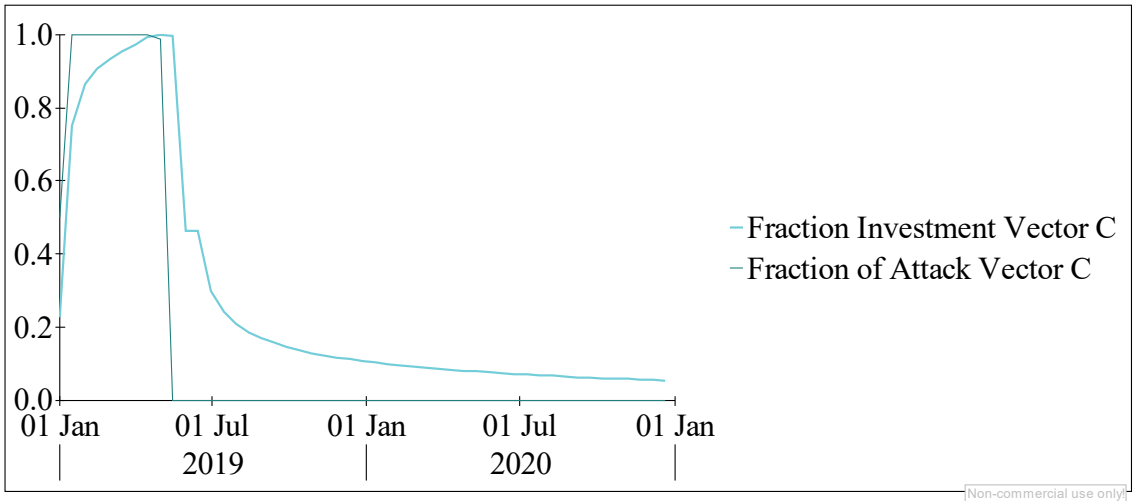

Fig. 13. The share of investments and the share of attacks on the vector *C*

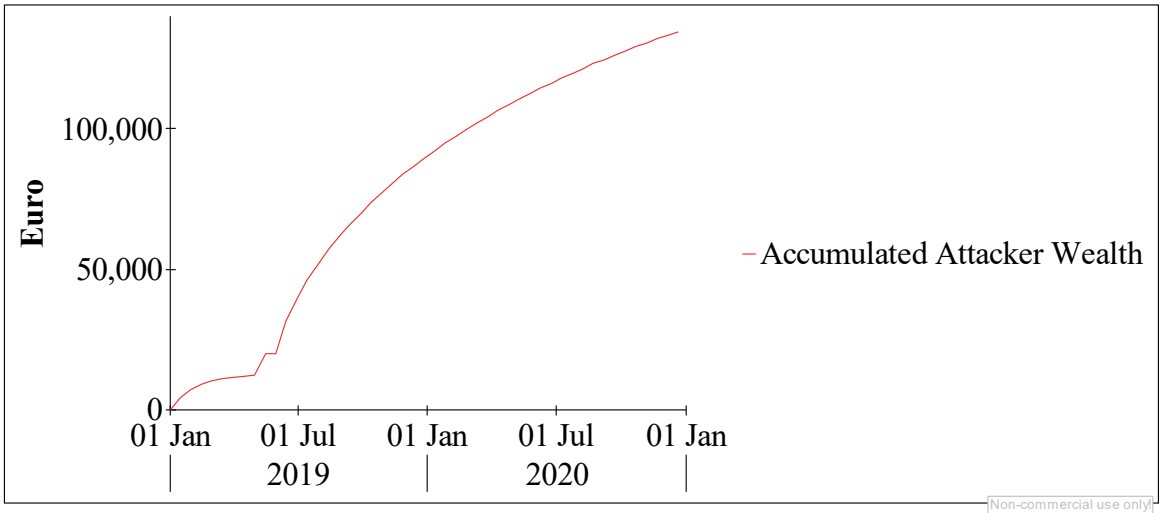

Fig. 14. The accumulated welfare of attackers

When changing the initial distribution of successful attacks on vectors ($A = 10$, $B = 10$, $C = 5$), it can be noted that the vulnerability of vector *C* remains negative (Fig. 15), and the number of successful attacks on this vector remains zero (Fig. 16).

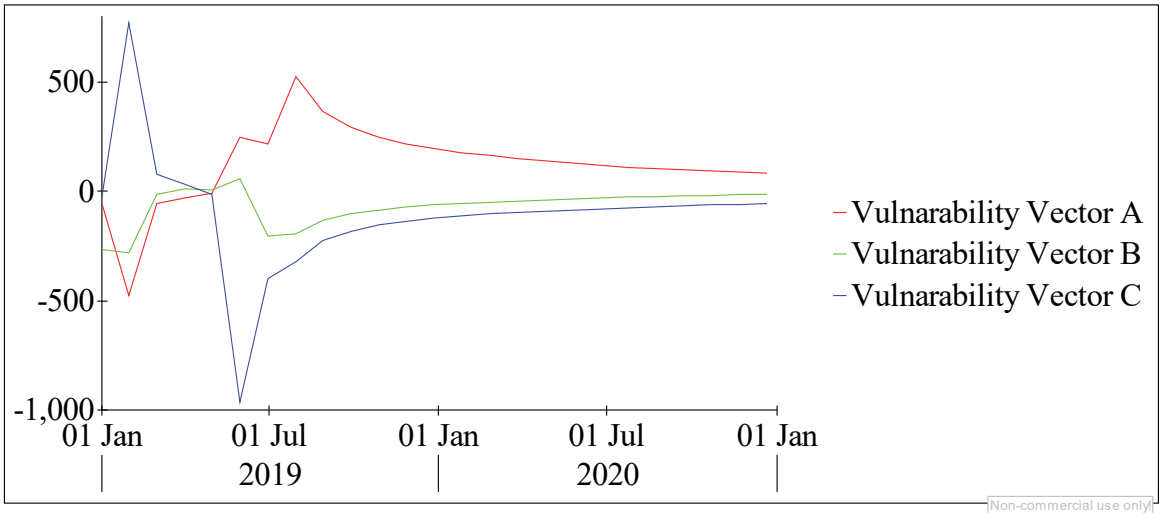

Fig. 15. Vulnerability of attack vectors

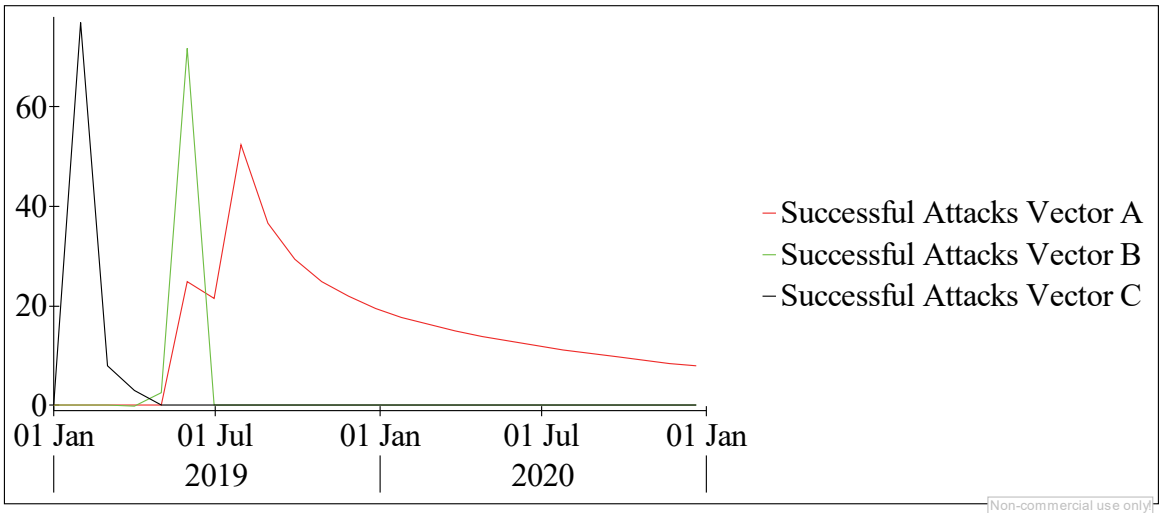

Fig. 16. Distribution of successful attacks by vectors

At the same time, there remains a general correspondence between the shares of successful attacks and the shares of investment funds according to attack vectors (Fig. 17–19).

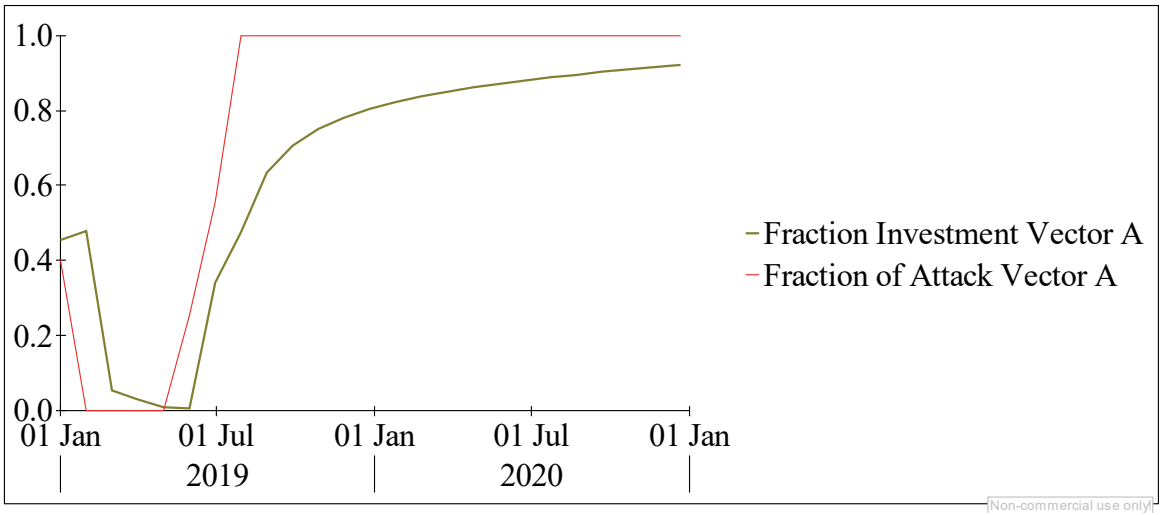

Fig. 17. The share of investments and the share of attacks on vector *A*

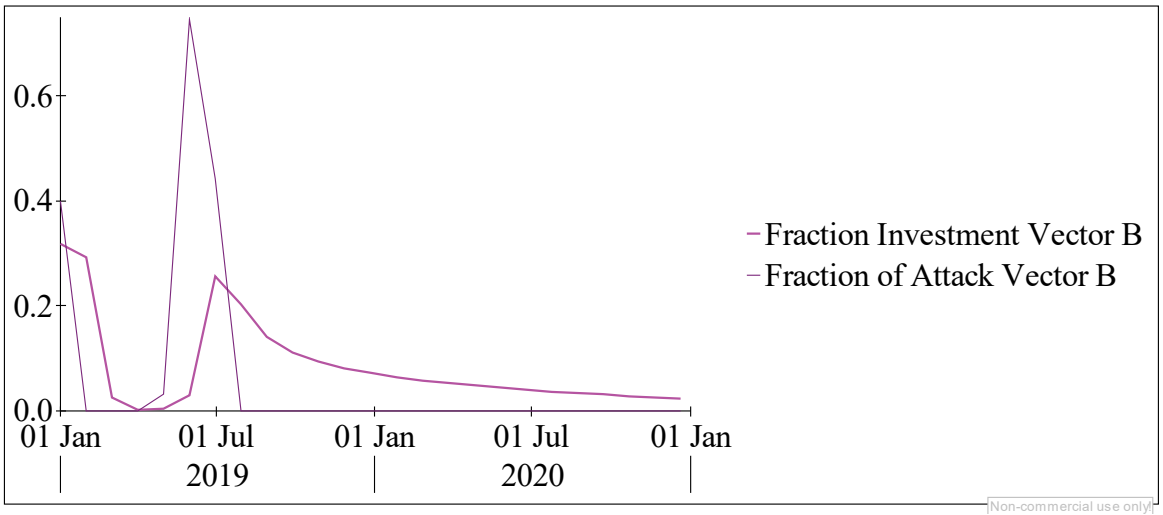

Fig. 18. The share of investments and the share of attacks on vector *B*

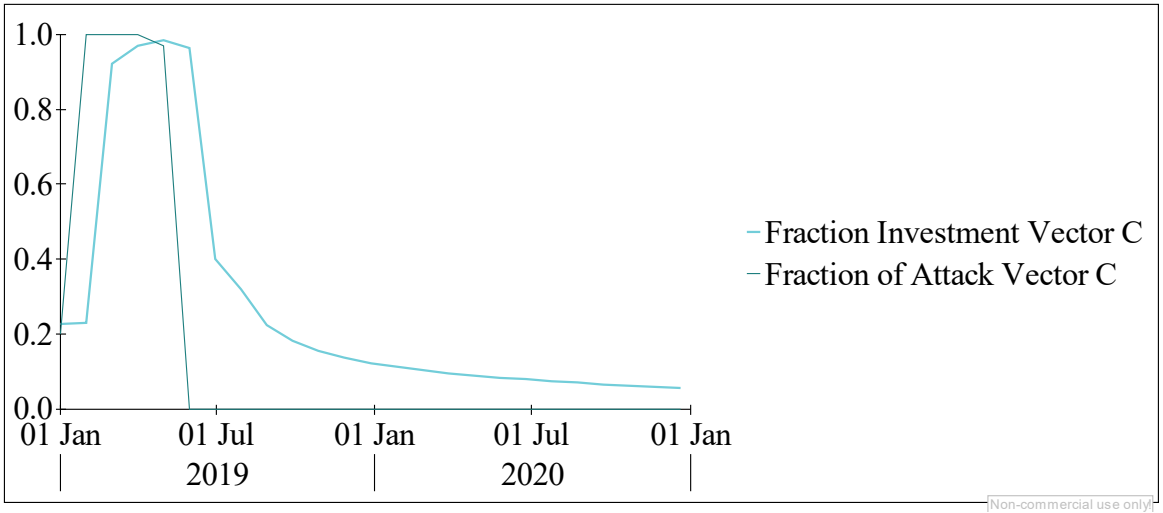

Fig. 19. The share of investments and the share of attacks by vector *C*

The overall dynamics of wealth accumulation by attackers does not change during the redistribution of funds for the implementation of attacks on various vectors (Fig. 14, Fig. 20).

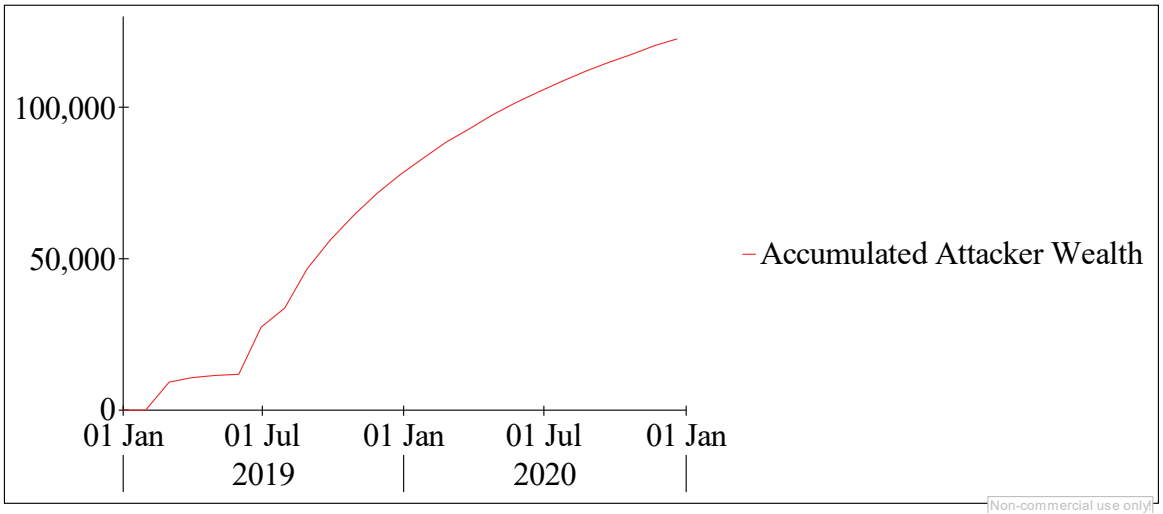

Fig. 20. Accumulated welfare of attackers

Similar results were obtained with the initial distribution of successful attacks by vectors, when the most successful attacks were carried out along vector *B*.

The results of the sensitivity test showed that the model is sensitive to the initial conditions for the accumulated successful attacks on vectors *A*, *B* and *C*. The results correspond to the behavior of a real system in accordance with the literature data.

Models of system dynamics are usually formulated in continuous time and are solved by numerical integration. The construction method chosen to build this model was of the Runge-Kutta 4th order (fixed step) with a time step equal to 0.25, which means that since the simulation is performed in months, attacks will be displayed at the time step, occurring weekly. These choices were made in such a way as to ensure the accuracy of the basic dynamics in accordance with the model's purpose.

The purpose of the **DT error test** is to determine if the model is sensitive to the time step settings. This test is performed by halving the time step from 0.25 to 0.125 and restarting the model. The result of this test demonstrated that the model is not sensitive to changes in DT.

Once sufficient confidence has been achieved in the reliability of the model structure, tests of model behavior are usually conducted to measure how accurately the model can reproduce the basic behavior models demonstrated by a real system. Typically, this test involves comparing the generated model behavior with the reference mode (real system behavior). However, the reference model for this study cannot be built due to the lack of available data. Instead, the context of model behavior was formed on the basis of the concepts existing in the literature regarding information security.

Conclusion

The article presents the developed system-dynamic model of antagonistic agents behavior under conditions

of cyber conflict. The model is a system of linear algebraic and differential equations, consisting of three submodels: defender, attacker and battlefield. For the developed model, a series of tests has been carried out that implement the model verification process. Verification of the model is based primarily on structural and structurally-oriented behavior tests. Testing of the behavior model was carried out on the basis of existing knowledge in the literature on information security. Nevertheless, the model successfully "passed" the validation test for all major tests and can be recognized as adequate to the behavior processes for the modeling of which it was created.

References

1. Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003a), Information security expenditures and real options: a wait-and-see approach, *Computer Security Journal*, No. 19(2), pp. 1-7.

2. Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003b), Sharing information on computer systems security: an economic analysis, *J. Account. Public Policy*, No. 22(6), pp. 461-485.

3. Anderson, R. (2001), Why information security is hard – An economic perspective, *Proceedings – Annual Computer Security Applications Conference, ACSAC*, pp. 358-365.

4. Gartner (2011), Magic Quadrant for Security Information and Event Management, *Gartner RAS Core Research.*

5. Gartner (2012), IT Key Metrics Data 2012: IT Enterprise Summary Report, *Gartner RAS Core Research.*

6. Suby, M. and Dickson, F. (2015), The 2015 (ISC) Global Information Security Workforce Study, *A Frost & Sullivan White Paper*, pp. 1-28, available at: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)?-Global-Information-Security-Workforce-Study-2015.pdf.

7. Whitman, M.E. (2003), Enemy at the Gate: Threats to Information Security, *Communications of the ACM*, No. 46(8), pp. 91-95. https://doi.org/10.1145/859670.859675.

8. Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016), Taxonomy of information security risk assessment (ISRA), *Computers & Security*, No. 57, pp. 14-30.

9. Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O., Salii, A., Timochko, O., Tiurin, V. and Yarovyi, A. (2019), Development of the model of the antagonistic agents behavior under a cyber conflict, *Eastern-Europe Journal of Enterprise Technologies*, Vol. 4, No. 9(100), p. 6-19.

10. Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015), The impact of information sharing on cybersecurity underinvestment: A real options perspective, *Journal of Accounting and Public Policy*, No. 34(5), pp. 509-519.

11. Kiely, L. and Benzel, T.V. (2006), Systemic security management, *IEEE security & privacy*, No. 4(6).

12. Tipton, H. and Krause, M. (2006), *Information Security Management Handbook: Fifth Edition*, Vol. 3, Auerbach Publications, Boston, MA, USA.

13. Huang, C.D. and Behara, R.S. (2013), Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints, *International Journal of Production Economics*, No. 141(1), pp. 255-268.

14. Barlas, Y. and Erdem, A. (1994), Output Behavior Validation in System Dynamics Simulation, *Proceedings of the European Simulation Symposium*, Istanbul, Turkey, pp. 81-84.

15. Sterman, J. (2000), *Business Dynamics. Systems Thinking and Modeling for a Complex World*, McGraw Hill Higher Education, Boston.

16. Gordon, L.A. and Loeb, M.P. (2002), The Economics of Information Security Investment, *ACM Transactions on Information and System Security*, No. 5(4), pp. 438-457.

17. Gordon, L.A. and Loeb, M.P. (2006), Budgeting process for information security expenditures, *Communications of the ACM*, No. 49(1), pp. 121-125.

18. Pindyck, R. (1991), Irreversibility, Uncertainty and Investment, *Journal of Economic Literature*, AA/A (September), pp. 1110-1148.

Список літератури

1. Gordon L.A. Information security expenditures and real options: a wait-and-see approach / L.A. Gordon, M.P. Loeb, W. Lucyshyn // Computer Security Journal. – 2003a. – № 19(2). – P. 1-7.

2. Gordon L.A. Sharing information on computer systems security: an economic analysis / L.A. Gordon, M.P. Loeb, W. Lucyshyn // J. Account. Public Policy. – 2003b. – № 22 (6). – P. 461-485.

3. Anderson R. Why information security is hard - An economic perspective / R. Anderson // Proceedings – Annual Computer Security Applications Conference, ACSAC. – January 2001. – P. 358-365.

4. Gartner. Magic Quadrant for Security Information and Event Management / Gartner // Gartner RAS Core Research. – 2011.

5. Gartner. IT Key Metrics Data 2012: IT Enterprise Summary Report / Gartner // Gartner RAS Core Research. – 2012.

6. Suby M. The 2015 (ISC) Global Information Security Workforce Study [Electronic resource] / M. Suby, F. Dickson // A Frost & Sullivan White Paper. – 2015. – P. 1-28. – Available at: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)?-Global-Information-Security-Workforce-Study-2015.pdf.

7. Whitman M.E. Enemy at the Gate: Threats to Information Security / M.E. Whitman // Communicationsofthe ACM. – 2003. – № 46(8). – P. 91-95. https://doi.org/10.1145/859670.859675.

8. Shameli-Sendi A. (2016). Taxonomy of information security risk assessment (ISRA) / A.Shameli-Sendi, R. Aghababaei-Barzegar, M. Cheriet // Computers & Security. – 2016. – № 57. – P. 14-30.

9. Milov O. Development of the model of the antagonistic agents behavior under a cyber conflict / O. Milov, S. Yevseiev, Y. Ivanchenko, S. Milevskyi, O. Nesterov, O. Puchkov, A. Salii, O. Timochko, V. Tiurin, A. Yarovyi // Eastern-Europe Journal of Enterprise Technologies. – 2019. – Vol. 4. – № 9(100). – P. 6-19.

10. The impact of information sharing on cybersecurity underinvestment: A real options perspective / L.A. Gordon, M.P. Loeb, W. Lucyshyn, L. Zhou // Journal of Accounting and Public Policy. – 2015. – № 34(5). – P. 509-519.

11. Kiely L. Systemic security management / L. Kiely, T.V. Benzel // IEEE security & privacy. – 2006. – № 4(6).

12. Tipton H. Information Security Management Handbook. Fifth Edition, Vol. 3 / H. Tipton, M. Krause. – Boston, MA, USA: Auerbach Publications, 2006.

13. Huang C.D. Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints / C.D. Huang, R.S. Behara // International Journal of Production Economics. – 2013.– № 141(1). – P. 255-268.

14. Barlas Y. Output Behavior Validation in System Dynamics Simulation / Y. Barlas, A. Erdem // Proceedings of the European Simulation Symposium, Istanbul, Turkey, 1994. – P. 81-84.

15. Sterman J. Business Dynamics. Systems Thinking and Modeling for a Complex World / J. Sterman. – Boston: McGraw Hill Higher Education, 2000.

16. Gordon L.A. The Economics of Information Security Investment / L.A. Gordon, M.P. Loeb // ACM Transactions on Information and System Security. – 2002. – № 5(4). – P. 438-457.

17. Gordon L.A. Budgeting process for information security expenditures / L.A. Gordon, M.P. Loeb // Communications of the ACM. – 2006. – № 49(1). – P. 121-125.

18. Pindyck R. Irreversibility, Uncertainty and Investment / R. Pindyck // Journal of Economic Literature. – 1991. – AA/A (September). – P. 1110-1148.

Received by Editorial Board 8.10.2019
Signed for printing 19.11.2019

Відомості про авторів:

Мілов Олександр Васильович
кандидат технічних наук доцент
Харківського національного економічного
університету ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0001-6135-2120

Пархуць Любомир Теодорович
доктор технічних наук професор
Національного університету "Львівська політехніка",
Львів, Україна
https://orcid.org/0000-0003-4759-9383

Мілевський Станіслав Валерійович
кандидат економічних наук доцент
Харківського національного економічного
університету ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0001-5087-7036

Погасій Сергій Сергійович
кандидат економічних наук доцент
Харківського національного економічного
університету ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0002-4540-3693

Information about the authors:

Oleksandr Milov
PhD in Technical Sciences Associated Professor
of S. Kuznets
Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0001-6135-2120

Lyubomyr Parkhuts
Doctor of Technical Science Professor
of Lviv Politechnic National University,
Lviv, Ukraine
https://orcid.org/0000-0003-4759-9383

Stanislav Milevskyi
PhD in Economics Associated Professor
of S. Kuznets
Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0001-5087-7036

Serhii Pohasii
PhD in Economics Associate Professor
of S. Kuznets
Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-4540-3693

ВЕРИФІКАЦІЯ МОДЕЛІ ПОВЕДІНКИ АНТАГОНІСТИЧНИХ АГЕНТІВ СИСТЕМ БЕЗПЕКИ

О.В. Мілов, Л.Т. Пархуць, С.В. Мілевський, С.С. Погасій

Верифікація моделі є дуже важливим кроком в методології моделювання поведінки антагоністичних агентів систем безпеки в цілому і системної динаміки зокрема. Під верифікацією моделі поведінки антагоністичних агентів будемо розуміти процес, що включає як формальні/кількісні інструменти, так і неформальні/якісні. У статті представлений процес створення моделі поведінки антагоністичних агентів. Попередньо сформовані припущення, що лежать в основі моделі, і обмеження створюваної моделі. Виділено складові моделі: підмодель захисника, підмодель атакуючого і підмодель середовища протистояння. Для кожної з підмоделей описані процеси і відносини, яка вона моделює, визначені змінні, використовувані для моделювання. Процеси і відносини між змінними представлені у вигляді системи лінійних і диференціальних рівнянь. За наведеною системи рівнянь математичної моделі побудована системно-динамічна модель взаємодії антагоністичних агентів. Показано, що для практичного використання програмної реалізації моделі поведінки обов'язковим є проведення процедури верифікації. Перераховані основні групи тестів, які необхідно виконати з використанням моделі, для підтвердження її адекватності умовам застосування і цілям, для досягнення яких вона була розроблена. Наведено результати тестування системно-динамічної моделі поведінки по основній групі тестів верифікації на кожному з трьох основних етапів перевірки моделі: структурні тести, структурно-орієнтовані тести поведінки і

тести моделей поведінки. З урахуванням отриманих результатів підкреслюється особлива важливість структурно-орієнтованих поведінкових тестів. Це сильні тести поведінки, які можуть надати інформацію про потенційні недоліки структури. Ці тести представляються найбільш перспективним напрямком для досліджень по верифікації моделей.

Ключові слова: *верифікація, модель поведінки, антагоністичні агенти, системно-динамічна модель, адекватність моделі.*

ВЕРИФИКАЦИЯ МОДЕЛИ ПОВЕДЕНИЯ АНТАГОНИСТИЧЕСКИХ АГЕНТОВ СИСТЕМ БЕЗОПАСНОСТИ

А.В. Милов, Л.Т. Пархуць, С.В. Милевский, С.С. Погасий

Верификация модели является очень важным шагом в методологии моделирования поведения антагонистических агентов систем безопасности в целом и системной динамики в частности. Под верификацией модели поведения антагонистических агентов будем понимать процесс, включающий как формальные/количественные инструменты, так и неформальные/качественные. В статье представлен процесс создания модели поведения антагонистических агентов. Предварительно сформированы предположения, лежащие в основе модели и ограничения создаваемой модели. Выделены составляющие модели: подмодель защитника, подмодель атакующего и подмодель среды противостояния. Для каждой из подмоделей описаны процессы и отношения, которая она моделирует, определены переменные, используемые для моделирования. Процессы и отношения между переменными представлены в виде системы линейных и дифференциальных уравнений. По приведенной системе уравнений математической модели построена системно-динамическая модель взаимодействия антагонистических агентов. Показано, что для практического использования программной реализации модели поведения обязательным является проведение процедуры верификации. Перечислены основные группы тестов, которые необходимо выполнить с использованием модели, для утверждения ее адекватности условиям применения и целям, для достижения которых она была разработка. Приведены результаты тестирования системно-динамической модели поведения по основной группе тестов верификации на каждом из трех основных этапов проверки модели: структурные тесты, структурно-ориентированные тесты поведения и тесты моделей поведения. С учетом полученных результатов подчеркивается особая важность структурно-ориентированных поведенческих тестов. Это сильные тесты поведения, которые могут предоставить информацию о потенциальных недостатках структуры. Эти тесты представляются наиболее перспективным направлением для исследований по верификации моделей.

Ключевые слова: *верификация, модель поведения, антагонистические агенты, системно-динамическая модель, адекватность модели.*