UDC 681.32:007.5
DOI: 10.15587/1729-4061.2019.181047

DEVELOPMENT OF THE INTERACTING AGENTS BEHAVIOR SCENARIO IN THE CYBER SECURITY SYSTEM

O. Milov
PhD, Associate Professor*
S. Yevseiev
Doctor of Technical Sciences, Senior Researcher*
E-mail: serhii.yevseiev@hneu.net
V. Aleksiyev
Doctor of Technical Sciences, Professor*
P. Berdnik
PhD
Department of Natural Sciences
V. N. Karazin Kharkiv National University
Svobody sq., 4, Kharkiv, Ukraine, 61022
O. Voitko
PhD, Head of Research Laboratory
Research Laboratory of Information Security Issues
Department of Information Technology and Information Security Employment
Institute of Information Technologies**
V. Dyptan
PhD, Associate Professor
Department of Air Force Logistics
Aviation and Air Defense Institute**
Y. Ivanchenko
PhD, Associate Professor
Department of Information Technology Security
National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, Ukraine, 03058
M. Pavlenko
Doctor of Technical Sciences, Professor, Head of Department
Department of Mathematical and Software of Automated Control Systems***
A. Salii
PhD, Associate Professor, Deputy Head of Institute
Aviation and Air Defense Institute **
S. Yarovyy
PhD
Department of Combat Use of Radar Armament***
*Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
**National University of Defense of Ukraine named after Ivan Chernyakhovsky
Povitroflotskiy ave., 28, Kyiv, Ukraine, 03049
***Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023

Представлені результати моделювання та аналізу сценаріїв поведінки взаємодіючих агентів в умовах кіберконфлікта. Представлені загальні підходи до розробки сценарію поведінки антагоністичних агентів. Наведено визначення сценарію і виділені фактори, що визначають сценарій поведінки. Наведені сценарії визначаються такими факторами як співвідношення можливостей атакуючої і захищається сторін, наявність або відсутність обміну інформацією між агентами системи безпеки, час перемикання на новий вектор атаки. Знайдено значення часу перемикання на новий вектор атаки, при якому взаємодія носить більш стійкий характер. Це свідчить про те, що реакція боку захисту не повинна бути чисто реактивної, а стратегія «чекай і дивись» не завжди є найкращою. Проведено моделювання та аналіз результатів в умовах обміну інформацією між агентами системи захисту і в умовах відсутності такого обміну. Відзначено переваги та недоліки такої поведінки. Показано, що при зміні часу перемикання на новий вектор атак змінюються не тільки фінансові показники діяльності учасників кіберконфлікта, а й характер взаємодії. Знайдено значення часу перемикання на новий вектор атаки, при якому взаємодія носить більш стійкий характер, що говорить про те, що реакція боку захисту не повинна бути чисто реактивною, а стратегія «чекай і дивись» не завжди є найкращою. Показано, як запропонований підхід можна використовувати для обґрунтування вибору стратегії поведінки агентів в системах безпеки, а також для економічних оцінок контрзаходів і їх стримуючого впливу на зловмисників. Пропоновані сценарії можна розглядати як корисний інструмент для оцінки інвестицій в безпеку контуру бізнес-процесів особами, які приймають рішення

Ключові слова: сценарний аналіз, сценарне моделювання, системи безпеки, поводження агентів, система кібербезпеки

Received date 11.09.2019
Accepted date 16.10.2019
Published date 28.10.2019

1. Introduction

The scenario approach to solving complex poorly formalized problems is gaining more and more popularity. The approach is actively used in dynamic and intelligent modeling systems, as well as a means of representing and structuring knowledge.

Solving the problems of ensuring the security of systems requires building forecasts of possible changes in their environment. There are two fundamental approaches to

forecasting: forecasting the future based on the past and forecasting the future, taking into account the emergence of new trends and events that might not take place in the past. Forecasts obtained in the first way usually have a statistical or theoretical justification, but they are not able to describe new situations. In contrast, the forecasts associated with the generation of hypotheses do not have a rigorous justification, but they provide an idea of new options for a possible future that have not been encountered in the past.

The first approach is widely used to predict large-scale phenomena, the description of which usually does not highlight active and unpredictable actors. The second approach is most often used to describe possible behaviors of systems containing active participants (players). One of the parties, having no information about the strategies of the opposing side, is forced to generate them on the basis of the knowledge available to it. The scenarios of the possible interaction of security system agents presented in the paper are the implementation of the second forecasting approach.

Especial popularity of scenario analysis in recent decades is primarily due to two interdependent factors. First, both at the practical and theoretical levels, the objective necessity of using a systematic approach to the study of critical infrastructure objects was recognized, one of the most important stages of which is modeling. Secondly, the pace of development of information technology and the penetration of the global network into ever new areas of human activity are increasing. These processes are accompanied by an increase in the number of cyber threats, which acquire the character of hybridity and synergy. And this, in turn, significantly complicates the functioning and development of any entities, significantly enhances the uncertainty of future performance.

The development and use of scenario analysis and modeling are one of the methods used in a systematic approach to studying the activities of security systems. This method ensures the normal functioning of business processes at any level and may turn out to be a tool that increases the overall level of security.

Scenario analysis is a risk management method, the main principle of which is to simulate possible situations and subsequent quantitative risk assessment based on the conclusions drawn from the modeling results. The main goal of scenario modeling is to identify the risks inherent in the corresponding business process (BP) circuit, determine the stability of the BP circuit to the consequences of risks, and support the cyber security toolset at an adequate level. Scenario analysis allows you to answer the question: "What if?".

2. Literature review and problem statement

In [1], a scenario is a description of a possible state of an object in the future, hypothetically or mathematically predicted. Moreover, the achievement of such a state should be preceded by the implementation of a certain combination of factors. The paper reveals the structure of the "scenario analysis" method, which consists in passing through several stages:

– representation of the investigated object as a model;

– allocation of key factors of influence and resulting criteria;

– definition of a rating scale;

– stress testing of the resulting model;

– analysis of an alternative series of behavioral characteristics of the model;

– synthesis of the results;

– testing on historical data (back testing);

– conclusion.

Despite the focus of the paper on the banking sector, it presents a number of general provisions applicable to any field of activity.

Based on a definition based on a broad understanding of the field, a typology of scenario analysis and modeling methods is proposed and discussed in [2]. Three "macro" characteristics are presented – goals, design and content – and ten "micro" characteristics in these broad categories. This typology demonstrates the diversity of scripting approaches, the ways and contexts in which they are used, and the results they produce.

It is noted that there are various definitions of a "scenario", but there is consensus on one point: this is not a forecast. Various definitions emphasize that they are: hypothetical, causal, internally consistent and/or descriptive. A definition is proposed that covers many of the characteristics proposed by other authors. Scenarios are sequential descriptions of alternative hypothetical options for the future that reflect different points of view on past, present and future events that can serve as the basis for action [3].

There are several typologies of scenarios, for example, those proposed in [4–8]. Each of them defines the fundamental differences between the types of scenarios. It is noted that the problem lies in the fact that typologies are often not able to cover the entire spectrum of modern development scenarios. The typology of Hagens and Van Osterhout [2] is later than [4], but less detailed. Business-oriented classifications, such as [5], do not take into account the differences between macroeconomic and environmental scenarios. Thus, we can conclude that the existing classifications are not detailed enough for in-depth analysis and not wide enough to justify the diversity of modern approaches to scenario development.

Currently, many types of scenario approaches are used, from research to decision-oriented and from intuitive to analytical. Scenarios show varying degrees of difficulty. There is no single "right" approach, and different contexts require different scenarios. The typology helps organize a variety of studies to pave the way through many possibilities, which helps to evaluate current scenario practice that can be used to determine the structure of the scenario process.

In [9], an attempt was made to investigate some of the problems that underlie scenario-oriented approaches, primarily in the development of requirements (RE) and to propose a structure for their classification. The classification structure is a four-dimensional platform that defines an approach by its form, content, purpose and life cycle. Each dimension in itself is multifaceted, and the metric is associated with each aspect. Motivation for developing a structure has three aspects:

– help to understand and clarify existing scenario-based approaches;

– identify industry practice scenarios;

– help researchers develop more innovative, scenario-based approaches.

The proposed structure of the scenarios suggests considering the scenarios in four different representations, each of which allows you to cover a specific relevant aspect of the scenarios. Each specific scenario will be characterized in accordance with these four views.

A form submission deals with a way to describe a scenario: are the scenarios described formally or informally, in a

static, animated, or interactive form? – These are questions about scenarios that are consistent with this view.

Content presentation refers to the kind of knowledge that is expressed in a script. Scenarios may, for example, focus on describing the functionality of a system, or they may describe a broader view in which functionality is embedded in a larger business process with various stakeholders and resources associated with it.

The target view is used to determine the role that the script should play in the requirements development process. A description of the system's functionality, exploring design alternatives, or explaining system weaknesses or inefficiencies are examples of roles that can be assigned to a script.

The life cycle view suggests that scenarios are considered as artifacts that exist and evolve over time through operations in the requirements development process. Creation, refinement, or deletion are examples of such operations. From this perspective, the issue of sustainability is also addressed.

The general conclusion arising from the analyzed paper can be formulated as follows. Scenario approaches are very complex, multidimensional objects and cannot be adequately represented only using simple classification methods based on predicates. Rather, there is a need for a four-dimensional structure of form, content, purpose and life cycle for the scenario approach, which will be well described in this case.

Each dimension in itself is multifaceted. To fix the position of the scenario approach, it is necessary to introduce a metric for each aspect. In general, the paper reflects a comprehensive set of characteristics that cover all aspects of the structure.

The application of a structure based on twelve approaches shows that they all have some properties that characterize the scenarios. Scenarios often refer to specific descriptions of situations or behaviors, focus on relevant contextual knowledge that reflects a point of view, and are open and informally expressed most of the time in natural language texts.

The practical application of the proposed script classification system has demonstrated certain difficulties associated with the lack of formal descriptions and technological parts of the approaches. In addition, the application of this approach has shown that there are differences in the points of view of researchers and practitioners. Methodological recommendations, script life cycle management, creating a text script are key issues in practice, while they are not sufficiently represented in the studies.

As software systems manage the growing amount of valuable and important information, software security is becoming a serious problem. In [10], a unified threat model was presented for the analysis and assessment of system threats at the design stage. However, another important issue is checking how the system under development copes with possible attacks at an early stage of design. Software security testing should focus on testing design models, not just implementation, to ensure that the developed system can protect the resource from attacks through risk reduction measures.

An approach based on an attack scenario for testing software security at the design stage was presented in [11]. Attack scenarios are created based on an extended action diagram (EAD) and a unified threat model (UTM). When creating attack scripts, an attack scheme and a security scheme were used to characterize a particular type of attack and means of counteracting it. Security test situations were automatically generated from attack scenarios based on various criteria. The approach was illustrated by the example of developing an online banking system. This approach can help designers test the system's response to potential attacks, and then improve the system design to meet the necessary security requirements at an early stage of design.

In [12], a classification of the types of modern terrorism is presented and scenarios and probabilistic models of ordinary, technological, and so-called intellectual terrorism are described. Scenarios are distinguished by their initiating events, distribution methods, damaging factors, probabilities and consequences. A comparative assessment of these three types of terrorism is presented. Dynamic tripartite models allow us to assess the situation from the point of view of terrorists and law enforcement agencies, administer a complex engineering system, and also analyze the actions and counteractions of various parties involved. A new integrated approach to ensuring the security of complex engineering systems is described. It should be noted that this approach is focused not only on the development of protective barriers and means of protection against a predetermined list of design scenarios of terrorist attacks, but also on increasing the system's resistance to attack scenarios that go beyond the scope of the design.

Complex engineering systems (CES), such as nuclear and thermal power plants; hydraulic structures; chemical, metallurgical and oil refineries; etc. are crucial from the point of view of life support of the population and ensuring sustainable economic development. The functioning of complex engineering systems is associated with the storage, processing and transportation of a huge amount of energy and hazardous materials. Unauthorized release of energy and hazardous materials in CES can lead to catastrophic consequences and cause cascading failures in interconnected infrastructures. This makes complex engineering systems attractive for cyber terrorists and requires special attention in countering terrorist threats [13–15].

Complex engineering systems are characterized by a complex structure, complex behavior and interaction between their components, which determine the ability of systems to redistribute loads and withstand cascading failures that occur after a local failure of their individual components. Due to the high level of uncertainty regarding the control parameters of CES, environmental conditions and external influences, the assessment of the characteristics of a complex engineering system should be probabilistic. For the stated reasons, it is proposed to describe the evolution of such systems by multidimensional scenario trees [16–18].

It is noted that knowledge bank is an effective means of providing protection from the effects of cyber terrorism. The knowledge bank should be used to analyze accidents and disasters in complex engineering systems, to study the scenarios with which they can be initiated. This should lead to a decrease in the vulnerability of CES with respect to attacks of various nature [19].

The knowledge bank should be used to analyze accidents and disasters in complex engineering systems.

The creation of such a bank should be based, first of all, on the development of a framework for the specification of script knowledge bases. Therefore, the work [20] is relevant. It is noted that this structure is able to support dynamic planning, execution and coordination of operations not so much for single defenders as for coalitions, which is relevant in the face of hybrid threats. The proposed solution is based on a formal grammatical structure, presented in matrix form, supplemented by an attribute component and using a sub-

stitution operation that allows a hierarchical specification of the scripting world. The proposed structure is illustrated by a coordinated multi-step attack on a computer network carried out by hackers.

The presented formal structure for the specification of scenario knowledge bases is integrated with an effective reasoning mechanism. The main ideas of this framework were first proposed in [21], and then developed in [22]. The framework is based on the use of a special form for representing context-free grammars. With some assumptions and simplifications within the framework of the considered class of applications, the structure allows various coalitions to dynamically (step by step) build consistent scenarios of their joint behavior. Scenario building depends on current intentions, coalition states achieved, and reactions from a potentially hostile and/or unpredictable environment. The main assumption made is that the set of actions used in the various scenarios is partially streamlined, and coordination is mainly designed to satisfy the partial order relationship imposed on the various actions of the coalition. In other words, a coalition can perform certain actions if and only if certain intermediate or final goals of other coalitions have already been achieved. Although the structure has certain limitations on the expressiveness of the scripting language, it can effectively solve a wide range of problems of dynamic development and coordination of the behavior of joint coalitions. It should be noted that coalition operations, along with computer support, are directed and controlled by human intelligence with a large number of common informal contexts and knowledge. Because of this, coordination within coalition operations requires much less expressiveness of the formal structure that defines this type of coordination. If such coordination is carried out in the agent community, then the general knowledge and context can be much poorer.

The knowledge and beliefs of a coalition are specified in terms of the knowledge of the scenarios presented below. Scenario knowledge formally represents a set of valid sequences of actions of coalitions involved in a joint operation. This knowledge, although formally presented, is used to dynamically derive an acceptable course of coordinated actions of coalitions, due to the current state of the scenario knowledge base, the goals achieved and the environmental response. The knowledge of the script is defined in terms of the following basic hierarchically ordered concepts: the model of simple behavior, the behavior model, the knowledge base of the script, and the mechanism for dynamically deriving the script.

The review allows us to draw certain conclusions and formulate the problem of the current work. First of all, it should be noted that the problem of constructing a theory of scenario analysis and modeling is relevant, although its development has been going on for more than a dozen years. At the same time, there is a certain gap between theoretical developments and the practical application of scenario analysis and modeling methods. On the other hand, the practical applications of scenario analysis and modeling methods largely depend on the characteristics of the object in relation to which they are applied. This is especially true for the business processes of security systems, which largely depend on the characteristics of the protected business processes and the features that cyberattacks take against them. Therefore, the main problem can be formulated as follows. It is necessary to develop scenarios for modeling and analyzing the behavior of interacting agents in security systems. Such scenarios should be based on the interaction model [23] developed in the framework of the previously formulated methodology [24].

3. The aim and objectives of the study

The aim of the study is to develop scenarios for the behavior of antagonistic agents in conditions of cyber conflict. Scenario modeling and subsequent analysis of the behavior of the parties to the cyber conflict should help determine the effectiveness of investing limited financial resources in selected areas. The resulting solution should ultimately lead to an increase in the level of security of critical infrastructure facilities.

To achieve this goal, it is necessary to accomplish the following objectives:

– to provide a general description of the behavior scenario, identifying the main factors and ranges of their changes that directly affect the adoption of investment decisions regarding protection against a particular attack vector;

– to develop scenarios for the interaction of the parties to the conflict and conduct scenario modeling, in order to determine the tolerant (satisfactory) values of factors that influence the adoption or change of previously made investment decisions;

– to perform an analysis of the results of scenario modeling and formulate an assessment of the effectiveness of the behavior of all parties to the conflict.

4. General description of the behavior scenario of interacting agents

The purpose of modeling and analyzing the behavior scenarios of interacting agents is to test a hypothesis, which can be formulated as follows. The wait and see (WAS) approach for defenders and the "weakest link" (WL) approach for attackers may not be effective strategies for making investment decisions in the face of uncertainty.

As the basis of scenario modeling, the conditions that determine the so-called basic run were considered [23]. These conditions imply, first of all, equality of opportunity for attackers and defenders and a certain basic value of the time to switch to another attack vector. The conditions for each scenario were formed on the basis of the basic run, the information asymmetry of the defender/attacker capabilities and the values of the security vector. These three conditions were chosen for the following reasons:

– firstly, the basic scenario shows the behavior of the system when the capabilities of the parties and the values of the value of the attack vectors are equal. This allows you to implement WL and WAS strategies both in the conditions of certainty and uncertainty in decision making;

– secondly, the capabilities of defenders and attackers determine how likely it is that attackers will use attack vectors as part of the WL strategy, and how likely it is that defenders will respond to violations based on the WAS strategy. If the attacker's resources are higher than that of the defender, he will be able to break the defense for various attack vectors. On the other hand, higher defenders capabilities mean that defenders will be able to block all incoming attacks. This means a lack of response to viola-

tions (since they are never implemented) and, therefore, the absence of a WAS strategy.

Finally, the asymmetry in the value of attack vectors gives the analysis greater realism, since in reality security vectors have different values of weighting factors that determine the value of the resource to which the corresponding attack is directed. Therefore, when violations occur along a vector with a greater weight, this can cause more or less damage to the defender's performance, depending on the value of such a vector.

The scripting space is a set of alternative conditions with respect to the conditions of the basic run. The specified space includes the conditions of the base scenario, asymmetric capabilities and values of the asymmetric vector relative to the base scenario with an uncertainty of zero and three levels of uncertainty, classified as low, medium and high uncertainty.

5. Development of scenarios for behavior modeling

The prevention of errors in organizing measures to counter cyber attacks, the detection of errors in choosing an inadequate method of countering attacks, and the resulting behavior of the opposing side at the stages preceding the implementation of the attack can significantly reduce the financial costs of organizing the protection of critical infrastructure from both conventional and hybrid attacks. The target setting that arises in this case consists in concentrating on the search for adequate behavioral patterns of conflicting agents in the face of possible cyber conflict, without waiting for its implementation.

For this purpose, methods and testing tools based on models have been actively developed recently, and the construction of various scenarios based on models is implemented using formal models and heuristic models. The resulting test scenarios are usually weakly associated with the specific features of the system in which they are planned to be used, but contain a representative set of situations from the point of view of the original model. This set of situations allows us to evaluate the results obtained using the existing model. Despite the fact that system implementations differ in their level of abstraction from their models, this approach allows us to automate the process of generating tests from the formal specifications of the system and significantly reduces the testing effort.

It should be noted that creating a formal description of systems is a very time-consuming process. Its complexity is due to several reasons. First of all, the construction of the initial model can be complicated by the incompleteness and variability of the initial requirements for the behavior of the system, and the resulting requirements for behavior scenarios. These difficulties force us to make constant changes in the formalization of the behavior of the warring parties, and as a result, cause significant time and financial costs in the implementation of security systems. Moreover, the requirements for performers of a relatively high level of necessary knowledge in the field of mathematical modeling are an additional limiting factor complicating the introduction of formal methods in the process of creating effective security systems for critical infrastructure facilities. It should be noted that at the moment there is a problem of the complexity of modern security systems, which leads to an explosive increase in the number of model states during its verification. The state of the model being tested includes a large number of variables and processes. Even if the number of processes is finite and the variables can take only a finite number of values, the total number of states can be very large. Considering that real security systems usually use parallel processes, the number of states of models of a parallel system grows exponentially with the number of components. Both the creation and analysis of the complete tree of behavior of the model of such a system are practically impossible.

The solution to these problems can be the use of scenario modeling, the principles and methods of which are clear to both a specialist in the field of security systems development and a specialist in the field of mathematical modeling. Modeling scenarios of behavior of security system agents, even if these scenarios are heuristic, semi-formal, allow us to give general assessments of the appropriateness of the behavior of one or another side of the conflict, being an intermediate link between informally formulated requirements and formal models presented in mathematical terms.

The scenarios illustrate the effect of changes in the capabilities of both sides and the weight inherent in each security vector on the financial performance of defenders and attackers and on successful attacks at various levels of uncertainty.

When activated, uncertainty is a single attack cost factor that determines the vulnerability of each security vector. To perform scenario space analysis, a continuous uniform distribution, also known as a rectangular distribution, was chosen.

The scenarios were analyzed taking into account the constant probability of increasing or decreasing damage from cyberattacks based on the minimum and maximum values at each level of uncertainty. The uniform distribution is given by the formula:

$$f(x)=\frac{1}{\max-\min},$$

where $\min<x<\max$.

The following ranges of uncertainty were proposed: low – [0.95, 1.1], medium – [0.875, 1.25] and high – [0.75, 1.5]. A variety of ranges of uncertainty will allow us to model and analyze more dynamic investment strategies for interaction between defenders and attackers. If we take the uncertainty value equal to 1, then in this case the defender is likely to close all the possibilities of a successful attack for the attacker.

Scenario 1 – basic.

The baseline scenario describes the initial conditions already referred to as the baseline run. Because the weak link approach works in all scenarios, attackers have historical successful attacks (A=100, B=70, and C=50). In this way, attackers access all subsequent attacks in accordance with these initial conditions. The following assumptions apply in the base case scenario:

– defenders and attackers have equal opportunities;

– the values of the security vectors are the same and equal to 1.

Uncertainty is a multiplier of the cost of a single attack. This means that there is no uncertainty in the basic scenario, since the uncertainty is 1. Both attackers and defenders know what damage (the cost of a single attack is assumed to be 10) the attack will inflict an information asset through a vector that is violated.

Running the baseline scenario shows that the attacks are successful, starting with A, as the initial period shows (Fig. 1). However, attackers switch to the next weakest link when the defender corrects security flaws and the attacker receives information about the most successful attacks (Fig. 2). The financial indicators of defenders and attackers in the absence of uncertainty are presented in Fig. 3.

In low-level uncertainty, the cost of a single attack is multiplied by uncertainty (value from the interval [0.95, 1.1]). Defenders' financials are still growing, albeit with slight fluctuations. On the other hand, the productivity of attackers is also steadily growing, but still weaker than that of defenders, as in the base scenario case.

Successful attacks are most likely due to the strategy of the weakest link of the attacker, showing an increase in the number of attacks for vectors B and A at the end of the period.

In case of uncertainty, the average level of the cost of a single attack is multiplied by a random amount of uncertainty from the interval [0.875, 1.25]. Defenders' financials fell below zero, while attackers continue to show positive results.

Successful attacks continue to hit the defense harder. This time, the vectors A, B, and C increase in size whenever the attacker switches to the next weakest link.

In this case, the cost of a single attack is multiplied by the amount of uncertainty from the interval [0.75, 1.5]. The financial performance of the defender continues to fall below zero, which is experiencing even greater financial losses. On the contrary, attackers still work positively and launch attacks more often (Fig. 4).

Under conditions of high uncertainty, all vectors experience successful attacks in different ways and with high intensity. The previous behavior makes the defender helpless in the sense that he cannot effectively allocate his resources, since successful attacks are constantly changing, which makes it difficult to follow the wait strategy (Fig. 5).

Scenario 2 – asymmetric capabilities.

The goal of this scenario is to show the behavior of modeled agents when one of the opponents has more resources than the other, and what is the impact of this behavior on successful attacks and financial results of both parties. The following are the assumptions considered in the asymmetric capability scenario:

– defenders' capabilities – 1000 units;

– attackers' capabilities are 100±20 (the reasons for the change in this range will be explained later);

– values of the security vectors are the same and equal to one.

In further modeling and analysis of the behavior of interacting agents, we will take into account that much more means are required to successfully repel an attack than to organize and conduct it. For the parameters used in the modeling of behavior scenarios, this ratio is approximately 10 to 1.

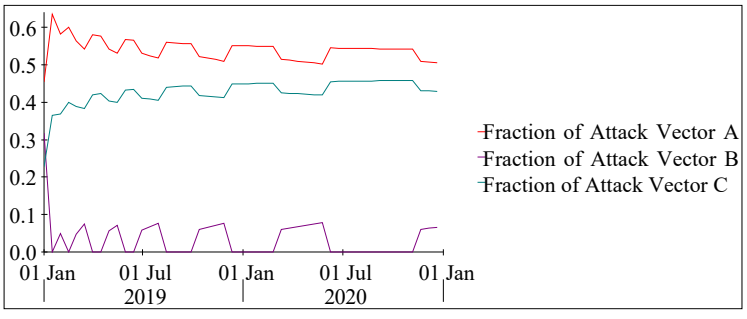

Fig. 1. Basic run. Distribution of attacks by vectors

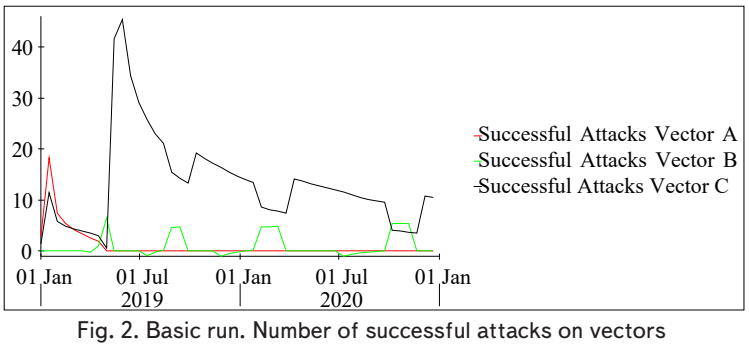

Fig. 2. Basic run. Number of successful attacks on vectors

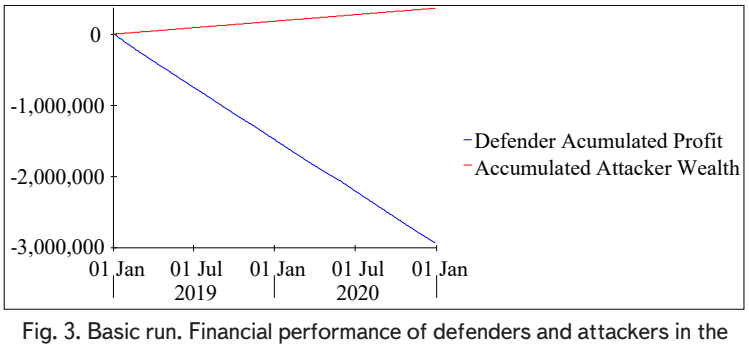

Fig. 3. Basic run. Financial performance of defenders and attackers in the absence of uncertainty

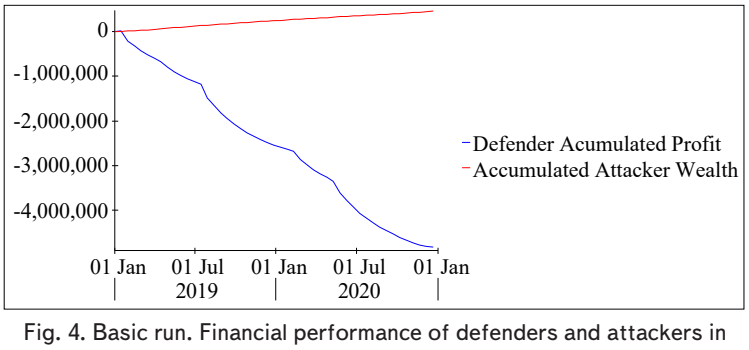

Fig. 4. Basic run. Financial performance of defenders and attackers in high uncertainty

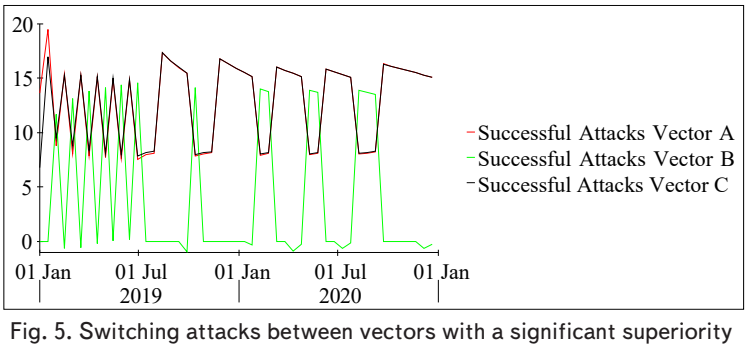

Fig. 5. Switching attacks between vectors with a significant superiority of attackers

If the defenders' capabilities significantly exceed the attackers' capabilities, successful attacks do not occur. On the contrary, when the capabilities of the attackers exceed a certain level corresponding to the limit level of possible reflection by defenders, attackers will constantly use all attack vectors. The distribution of attacks by vectors corresponds to the proportion with which they began to attack, since the defender cannot repel these attacks. This situation, as shown by simulation experiments, persists even when there is uncertainty at all its levels (Fig. 6).

Of particular interest is the behavior of interacting agents at the intersection of the marked level.

With an attacker-defender capability ratio of 125:1000, attackers' capabilities are enough to conduct successful attacks on all vectors. At the same time, switching between attack vectors takes place quite intensively, which does not allow the defense side to respond in a timely manner, identify and protect the weakest link (Fig. 5). This corresponds to the base run (Fig. 1–5).

With an attacker-defender capability ratio of 109:1000, the situation begins to change and a period arises at the initial moment when the defender's performance even exceeds the attackers' performance (Fig. 7).

The performance of the attackers is still higher than the performance of the defenders, however, manifestations of a change in the situation are already observed (Fig. 8).

The dynamics of the conduct varies with a capability ratio of 97:1000. And as the proportion decreases, the picture becomes clearer. There comes a turning point, when the defenders are able to repel more attacks, and this moment comes earlier (Fig. 9).

With a ratio of 93:1000, the defender no longer suffers financial losses from attacks (Fig. 10).

With a further change in the ratio of capabilities of the interacting parties (ratio 92: 1000), a situation occurs when all attacks are reflected (Fig. 11).

The obtained ratios allow us to estimate the necessary level of investment in cyber defense to partially or completely block attacks on the system. It can be assumed that the relations obtained (when setting up the model for specific values of the interaction parameters under the conditions of cyberattacks) can be used to assess the capabilities of the attack side, based on the available means of defense and the dynamics of attack reflection.

The following behaviors of interacting agents can be considered corporate security management strategies. An exchange of information may be considered as one of the proposed policy options. This policy option aims to reduce attack uncertainty and increase defense effectiveness. As a second policy option, a behavior scenario is considered in which the time to stop the attack changes, which is aimed at improving the defenders' knowledge of the attacks and increasing their financial performance.

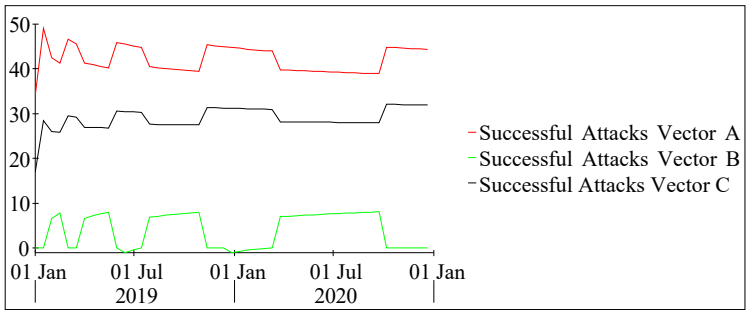

Fig. 6. Distribution of successful attacks by vectors in case of insufficient means of protection

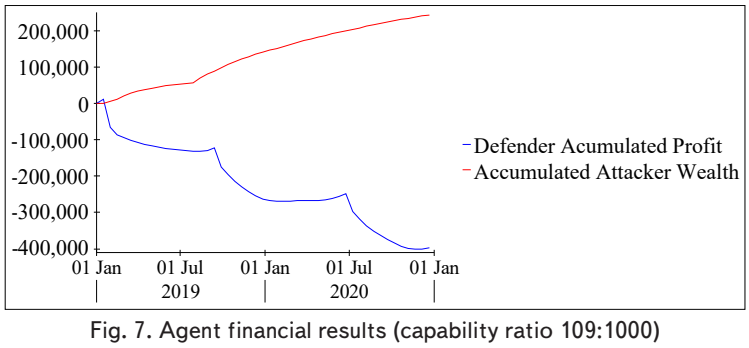

Fig. 7. Agent financial results (capability ratio 109:1000)

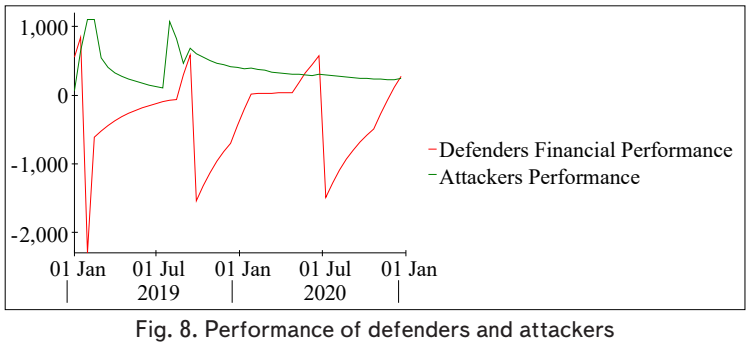

Fig. 8. Performance of defenders and attackers (capability ratio 109:1000)

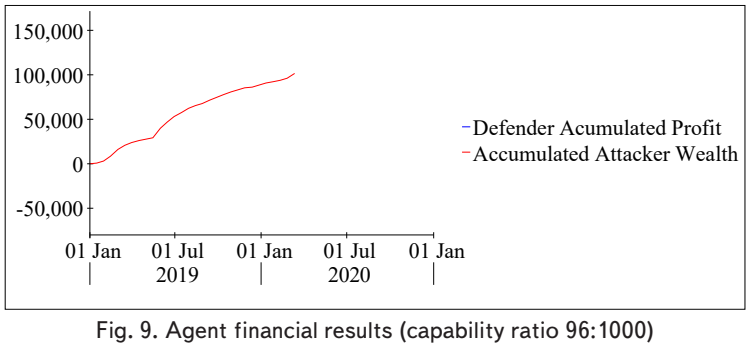

Fig. 9. Agent financial results (capability ratio 96:1000)

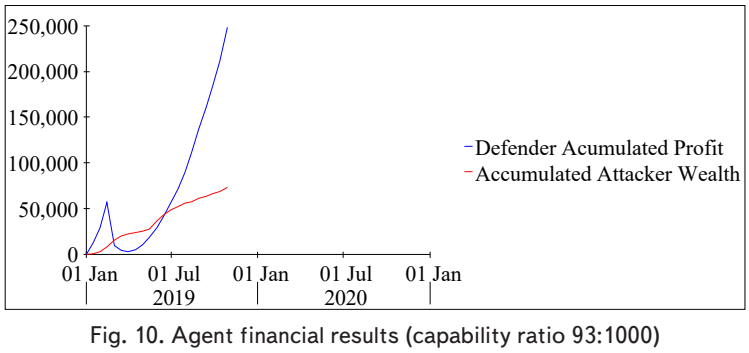

Fig. 10. Agent financial results (capability ratio 93:1000)

Scenario 3 – Exchange of information.

One of the economic barriers to improving information security is the lack of available data. Therefore, the argument for sharing information is based on the belief that firms can reduce uncertainty about threats based on the experience of other (especially similar) firms [25].

The analysis of policy options is modeled with the initial conditions of the basic run and compared with the simulations generated by adding an information exchange policy parameter to the model.

The exchange of information reduces the uncertainty affecting all processes of agent interaction. Therefore, it should be expected that, in the absence of uncertainty, the existence of an information exchange policy option will not affect the financial performance of defenders and attackers. Also, there are no changes in the dynamics of successful attacks when using an information exchange policy. Consequently, the behavior of the system remains the same as in the base scenario case (Fig. 12).

The use of low-level uncertainty also does not produce a significant effect, since the exchange of information already reduces uncertainty and significantly improves the financial performance of the defender. Meanwhile, the attackers' performance remains unchanged. It should be noted that as uncertainty grows, the financial performance of the defenders improves, surpassing the attackers at the end of the simulation. Defenders repel a portion of the attacks being undertaken and are able to recover from successful attacks.

With high uncertainty, the financial performance of the defenders decreases at the beginning of the simulation. Then the defenders adapt to the attack parameters and their financial results begin to exceed the results of the attackers (Fig. 13).

The effect of information exchange is also visualized in successful attacks, the offset of the attack along the vectors is reduced, which allows defenders to eliminate security vulnerabilities and gain advantages. However, in order for defenders to experience these benefits, they need to wait until this policy option reduces uncertainty.

The exchange of information can reduce uncertainty regarding investment decisions in the field of information security. As a result of this reduction in uncertainty, information exchange is likely to reduce the general tendency of firms to wait for a serious breach of information security before investing heavily in security activities. In other words, information exchange encourages firms to be more proactive than a reactive approach to investing in cybersecurity. Thus, the value of a wait-and-see approach decreases with increasing uncertainty associated with investments.

Firstly, it was illustrated that, in conditions of medium and high uncertainty, the financial performance of the defender behaves worse than ever with respect to their recovery from security breaches. This suggests that defenders must be patient in order to take advantage of information exchange, this conclusion makes sense, since it takes time to collect information. In addition, this information takes time for analysis and understanding by security personnel and for security managers to make investment decisions. In addition, the increase in protection benefits should encourage firms to provide information about attacks against them and the success of repelling attacks in exchange for receiving information from other firms. It can also offset the costs typically associated with belonging to an information exchange group [26].

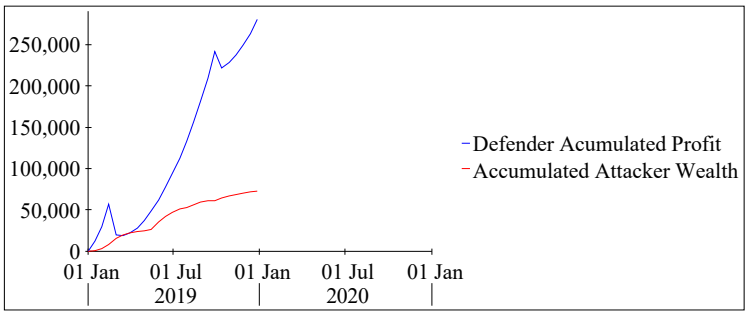

Fig. 11. Agent financial results (capability ratio 92:1000)

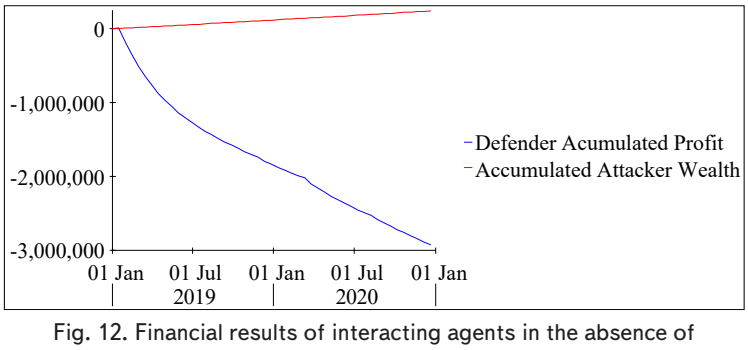

Fig. 12. Financial results of interacting agents in the absence of information exchange

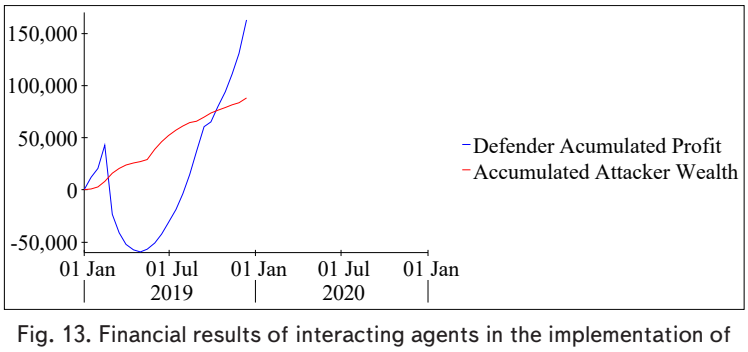

Fig. 13. Financial results of interacting agents in the implementation of information exchange

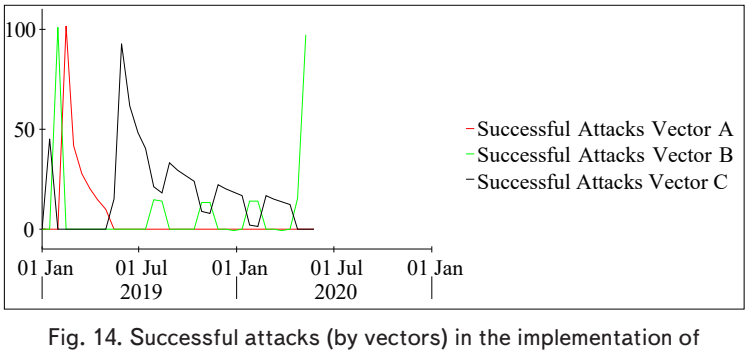

Fig. 14. Successful attacks (by vectors) in the implementation of information exchange

Analysis of the study showed that the exchange of information really offers the potential to reduce the overall uncertainty associated with information security. However, there are some pitfalls that may well hinder the realization of all po-

tential benefits. One of these pitfalls is the presence of free participants in the information exchange group. The emergence of free access in the information exchange group is one of the main reasons why companies do not want to share information about cybersecurity [27].

The free-rider problem refers to a situation where a firm can benefit from a situation, regardless of its contribution. An analysis of how the free-rider problem affects decisions to invest in cybersecurity is presented in [28, 29].

Another obstacle to sharing cybersecurity information for a firm is that it risks jeopardizing its own competitive advantage by exposing security flaws. Accordingly, in [26, 27] it is noted that the pitfalls of information exchange are related to the need to create economic incentives to facilitate the effective exchange of information, such as risk premium, error problem and generosity, etc.

Scenario 4 – Increasing the time of switching between attacks

Defenders make investment decisions based on data on successful attacks. This means that the attacks must be stopped after a while, either because they were repelled, or attempts are being made to find another vulnerability in the protection system.

The main goal of this scenario is to increase the time to switch to another attack vector. Therefore, the defender "stores" reports of successful attacks for a longer time in order to extract more information from them and ultimately reduce the uncertainty associated with future attacks. The change in the dynamics of successful attacks by vectors when changing the time of switching between attacks is shown in Fig. 15–17.

Attention should be paid to the decrease in the growth rates of financial indicators of cybercriminals with an increase in the time of switching between the vectors (Fig. 18–20). Moreover, with an increase in switching time to 4, a tendency is formed for the growth of financial indicators of defenders (Fig. 20).

Combining the two policy options, you can see in the previous diagrams that the overall improvement is seen from the defense side. Defenders' financial performance is significantly higher than that of attackers, and increasing and successful attacks in most cases are mitigated by the defender during periods, especially in conditions of high uncertainty.

Increasing the cessation of successful attacks has managerial implications. For example, by storing information on recorded successful attacks for 4 months instead of 1 month, firms may need specialized personnel to analyze the data collected and the response team (IT Forensics). In addition, the costs of data warehouse infrastructure and integrated data collection system are increasing.

If there is no uncertainty, the defender can still work well, following the standard approach of expectation and observation. As soon as uncertainty arises, the more valuable is the information obtained as a result of the observed attacks. This means that defenders become more active when uncertainty is high.

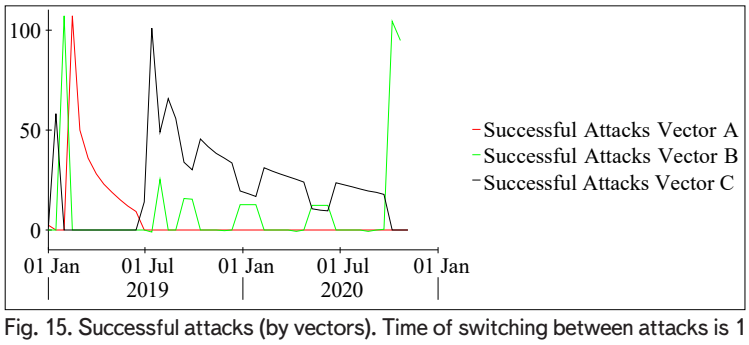

Fig. 15. Successful attacks (by vectors). Time of switching between attacks is 1

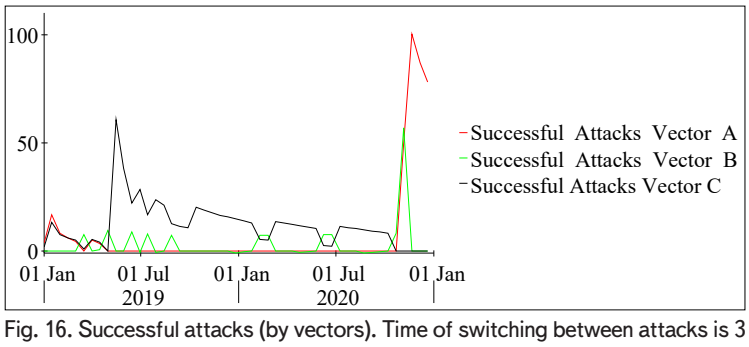

Fig. 16. Successful attacks (by vectors). Time of switching between attacks is 3

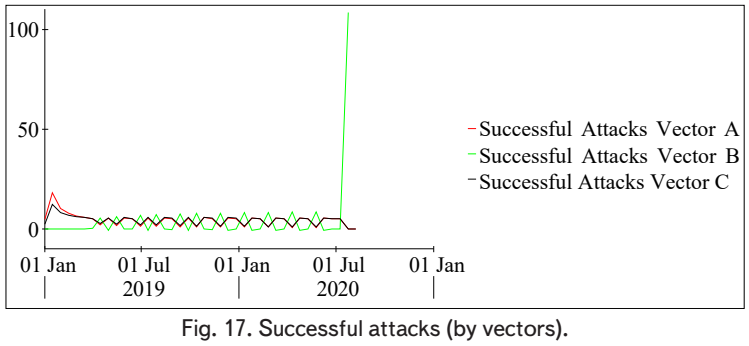

Fig. 17. Successful attacks (by vectors). Time of switching between attacks is 4

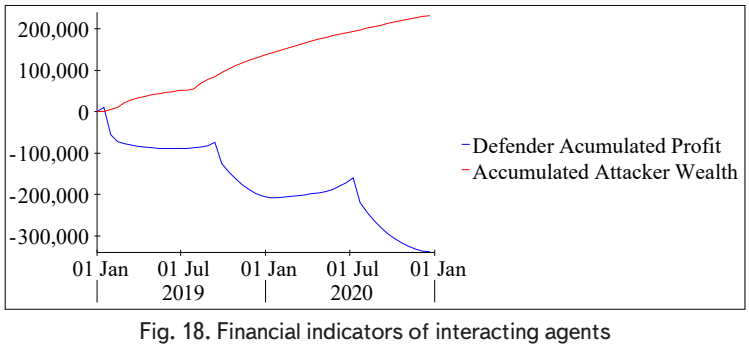

Fig. 18. Financial indicators of interacting agents (time of switching between vectors is 1)

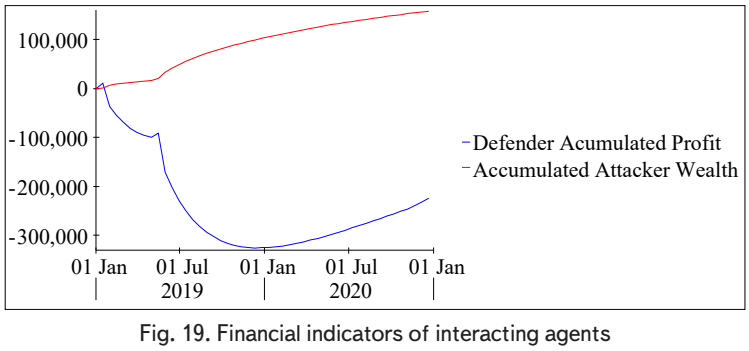

Fig. 19. Financial indicators of interacting agents (time of switching between vectors is 3)

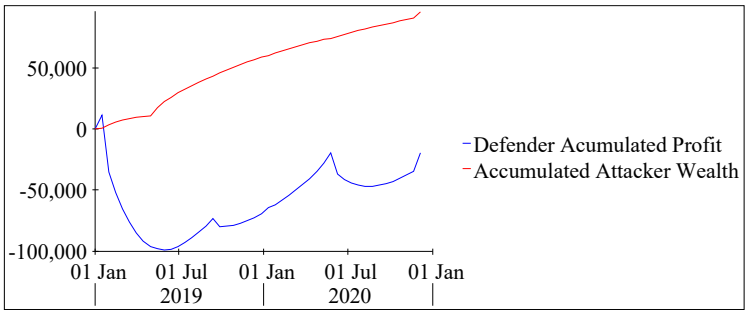

Fig. 20. Financial indicators of interacting agents (time of switching between vectors is 4)

6. Discussion of the results of scenario modeling and assessment of the effectiveness of the functioning of the parties to cyber conflict

The use of simulation methods, using the scenario approach and system dynamics methods, allows you to implement the following basic capabilities necessary to describe such a complex spatially distributed and dynamically changing phenomenon as cyber attacks and counteraction to them:

– the ability to describe the behavior of agents involved in the confrontation, processes implemented by the parties to the conflict, or cyber conflict as a whole at a high level of detail;

– the absence of restrictions between the parameters of simulation modeling, the state of the external environment of the real process and the simulated system;

– the ability to study the dynamics of cyber conflict, its individual agents and the process of its development as a whole in time and space;

– the ability to take into account the influence of the simulated system as providing the information subsystem on the efficiency of the security system as a whole.

The simulation of the behavior of the parties to the cyber conflict in the framework of the scenario approach allows us to formulate the following results.

Since the weakest link strategy works in all scenarios, an attacker will prefer the least secure vector and use it until he gets more advantages over other vectors. Meanwhile, the defender uses a wait-and-see strategy to eliminate vulnerabilities in accordance with successful attacks. This is effective when there is no uncertainty in the model.

As uncertainty arises and/or increases, the benefits of a wait-and-see approach decrease. Thus, in conditions of high uncertainty, the defender acts almost blindly, since violations are extremely unstable, this prompts the defender to postpone investments (or invest insufficiently) and agree that part of the attacks will be successful. This difficulty in making decisions negatively affects the reputation, and therefore the financial performance of the defender. The higher the uncertainty, the less intense the attacks in one direction with respect to the other. This means that the defender is investing in other vectors.

On the other hand, attackers can change the attack strategy. That is, they may not want to make wide use of the weakest link to confuse the defender and provoke the wrong distribution of investments in security. In fact, there is some evidence that some spammers send messages without any obvious purpose, other than overloading self-learning spam filters [30]. In this case, attackers can switch from one attack vector to another without using it completely.

Individually, each of the scenarios improves the defenders' financial performance over time. On the one hand, the exchange of information reduces uncertainty. On the other hand, it entails a later success than increasing the time to stop the attacks. At the same time, financial indicators of defenders in the conditions of information exchange suffer losses in the initial period of the scenario. Also, the exchange of information carries several obstacles that must be implemented in the first place. This is a free-rider problem and the lack of economic incentives for belonging to an information exchange group. The latter is explained by the fact that most firms hesitate to identify weaknesses in the security of their competitors, citing an unfavorable market position, even if a coordinated approach to attacks can lead to a faster reduction of risks for everyone.

Meanwhile, increasing the cessation time of attacks is in itself an almost immediate success, allowing you to deeply analyze the reported successful attacks for a longer time. This policy clearly improves financial performance for defenders and reduces the number of successful attacks. This policy option includes a large resource requirement. These resources are explained by the integrated infrastructure and specialized response personnel to collect, analyze and store information about the attacks for 4 months.

The implementation of a combination of information exchange and increasing the time to switch to a new attack vector depends on the size of firms and the available budget (opportunities) for investing in information security. In a combined policy simulation, combining the two policies has a small added value, since defenders can perceive the benefits differently by implementing only one policy at a time. The results of the scenario of changing the time of switching to another attack vector seem to be as good as the combined policy of using two scenarios. In other words, the marginal benefit of sharing information is almost zero if termination policy is already in place.

Thus, smaller firms may prefer to be part of an information exchange group, especially if they are similar firms, since less money is required to reduce uncertainty. The greater the similarities between firms, the greater the likelihood that the exchange of information will be accurate and valuable in terms of reducing uncertainty. Larger firms, on the other hand, may be motivated to introduce a stricter policy to end attacks, as they are more likely to have a higher budget to implement this policy. In addition, large firms can avoid the pitfalls of being part of an information exchange group and protecting their overall reputation.

The use of simulation modeling of hostilities in cyberspace can be recommended in the following cases:

– in the process of researching the features of the development of cyber conflict, when there is no complete statement of the research problem. In this case, the simulation model serves as a means of studying the phenomenon;

– when using analytical methods, but the mathematical processes that support them are complex and time-consuming, and simulation modeling provides an easier way to solve the problem;

– under conditions of monitoring the behavior of cyber conflict agents for a certain period when, if necessary, obtaining an assessment of the influence of parameters (variables) of a process or system;

– when it is impossible to observe phenomena in real conditions; when simulation is the only way to study a complex system;

– in conditions of monitoring the course of processes or the behavior of systems by slowing down or accelerating phenomena during simulation;

– during the training of specialists, when the simulation models provide the opportunity to acquire skills to repel cyberattacks;

– when studying new situations in real confrontation processes in cyberspace. In this case, simulation serves to test new strategies and rules for conducting experiments.

However, the scenario approach using simulation of combat operations along with advantages has some disadvantages, the main of which are the following:

– it may turn out that the model of cyber conflict described by the scenario is inaccurate, but the researcher is not able to assess the degree of this inaccuracy;

– the formation of stereotypes and patterns in assessing the situation in the context of cyber operations.

7. Conclusions

1. A general description of the scenario of behavior is formulated and the main factors that influence the decision-making on the direction of investments to protect against a particular attack vector are identified. The ranges of changes in the identified factors are determined. The highlighted factors were used as what-if variables in scenario modeling.

2. 4 scenarios of interaction between the parties to the conflict were developed and scenario modeling was carried out in order to determine the tolerant (satisfactory) values of factors that influence the adoption or change of previously adopted investment decisions. The following scenarios were presented: the basic scenario, the scenario of behavior under asymmetric capabilities of the parties to the conflict, the scenario of information exchange and the scenario of changing the time of switching between attacks. The main possibilities of the scenario approach using simulation methods are formulated. The advantages and disadvantages of the method arising from the results of simulation experiments are noted.

3. The analysis of the results of scenario modeling is carried out and an assessment of the effectiveness of the behavior of all parties to the conflict is formulated. In particular, the ranges of changes in the ratio of defenders and attackers' funds are determined. The ranges are determined by the conditions under which it is impossible to repel attacks, it becomes possible after a short adaptation of agents, or full protection is provided for the business process circuit and the moment of the onset of cyber conflict. An increase in the defenders' effectiveness in the case of information exchange in the presence of high uncertainty is demonstrated. Obstacles to using such a strategy are noted. The time of switching to protection from a new attack vector is determined, at which not only an increase in the financial performance of the defense system is achieved, but also the stability of behavior when opposing attacks on various vectors is increased.

References

1. Kovalev, P. P. (2009). Stsenarniy analiz, metodologicheskie aspekty. Finansy i kredit, 44 (380), 9–13.
2. Van der Heijden, K., Bradfield, R., Burt, G., Cairns, G., Wright, G. (2002), The Sixth Sense: Accelerating Organizational Learning with Scenarios. Wiley & Sons, 320.
3. Van Notten, Ph. (2005). Writing on the Wall: Scenario Development in Times of Discontinuity. Dissertation.Com., 228.
4. Ducot, G., Lubben, G. J. (1980). A typology for scenarios. Futures, 12 (1), 51–57. doi: https://doi.org/10.1016/s0016-3287(80)80007-3
5. Duncan, N. E., Wack, P. (1994). Scenarios designed to improve decision making. Planning Review, 22 (4), 18–46. doi: https://doi.org/10.1108/eb054470
6. Godet, M. (1997). Scenarios and Strategies: A Toolbox for Scenario Planning. Conservatoire National des Arts etMetiers (CNAM).
7. Godet, M., Roubelat, F. (1996). Creating the future: The use and misuse of scenarios. Long Range Planning, 29 (2), 164–171. doi: https://doi.org/10.1016/0024-6301(96)00004-0
8. Heugens, P. P. M. A. R., van Oosterhout J. (2001). "To boldly go where no man has gone before: integrating cognitive and physical features in scenario studies. Futures, 33 (10), 861–872. doi: https://doi.org/10.1016/s0016-3287(01)00023-4
9. Rolland, C., Ben Achour, C., Cauvet, C., Ralyté, J., Sutcliffe, A., Maiden, N. et. al. (1998). A proposal for a scenario classification framework. Requirements Engineering, 3 (1), 23–47. doi: https://doi.org/10.1007/bf02802919
10. Li, X., He, K. (2008). A Unified Threat Model for Assessing Threat in Web Applications. International Journal of Security and its Applications, 2 (3), 25–30.
11. Li, X., He, K., Feng, Z., Xu, G. (2014). Unified threat model for analyzing and evaluating software threats. Security and Communication Networks, 7 (10), 1454–1466. doi: https://doi.org/10.1002/sec.599
12. Reznikov, D. O., Makhutov, N. A., Akhmetkhanov, R. S. (2018). Analysis of Terrorist Attack Scenarios and Measures for Countering Terrorist Threats. Probabilistic Modeling in System Engineering. doi: https://doi.org/10.5772/intechopen.75099
13. Makhutov, N., Baecher, G. (Eds.) (2012). Comparative Analysis of Technological and Intelligent Terrorism Impacts on Complex Technical Systems. Amsterdam: IOS Press BV.
14. Countering Terrorism: Biological Agents, Transportation Networks, and Energy Systems: Summary of a U.S.-Russian Workshop (2009). Washington: The National Academies Press, 244. doi: https://doi.org/10.17226/12490
15. Frolov, K. V., Baecher, G. B. (Eds.) (2006). Protection of Civilian Infrastructure from Acts of Terrorism. NATO Security through Science Series. Springer. doi: https://doi.org/10.1007/1-4020-4924-2

16. Berman, A. F., Nikolaychuk, O. A., Yurin, A. Y. (2012). Intellectual data system for analyzing failures. Journal of Machinery Manufacture and Reliability, 41 (4), 337–343. doi: https://doi.org/10.3103/s1052618812040036
17. Makhutov, N. A., Reznikov, D. O. (2012). Analysis and ensuring protection of critical infrastructures taking into account risks and limit states. Problemy bezopasnosti i chrezvychaynyh situatsiy, 5, 14–36.
18. Makhutov, N. A., Reznikov, D. O., Zatsarinny, V. V. (2014). Two types of failure scenarios in complex technical systems. Problemy bezopasnosti i chrezvychaynyh situatsiy, 2, 28–41.
19. Bezopasnost' Rossii. Pravovye, sotsial'no-ekonomicheskie i nauchnotehnicheskie aspekty. Kosmicheskie sistemy i tehnologii povysheniya bezopasnosti i snizheniya riskov (2017). Moscow: MGOF «Znanie», 608.
20. Trotsky, D. V., Gorodetsky, V. I. (2009). Scenario–based knowledge model and language for situation assessment and prediction. SPIIRAS Proceedings, 8, 94–127. doi: https://doi.org/10.15622/sp.8.6
21. Tarakanov, A. (1988). Matrichnyy metod avtomaticheskogo sinteza programm. Izvestiya VUZov. Priborostroenie, 31 (10), 21–25.
22. Gorodetski, V. I., Tarakanov, A. O. (1996). Matrix Form of Attributive Grammars for Distributed Processing Planning and Control. Intelligent Control, Neurocomputing and Fuzzy Logic, 2.
23. Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O. et. al. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. Eastern-European Journal of Enterprise Technologies, 4 (9 (100)), 6–19. doi: https://doi.org/10.15587/1729-4061.2019.175978
24. Milov, O., Voitko, A., Husarova, I., Domaskin, O., Ivanchenko, Y., Ivanchenko, I. et. al. (2019). Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems. Eastern-European Journal of Enterprise Technologies, 2 (9 (98)), 56–66. doi: https://doi.org/10.15587/1729-4061.2019.164730
25. Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. Journal of Accounting and Public Policy, 34 (5), 509–519. doi: https://doi.org/10.1016/j.jaccpubpol.2015.05.001
26. Gal-Or, E., Ghose, A. (2005). The Economic Incentives for Sharing Security Information. Information Systems Research, 16 (2), 186–208. doi: https://doi.org/10.1287/isre.1050.0053
27. Gordon, L. A., Loeb, M. P., Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, 22 (6), 461–485. doi: https://doi.org/10.1016/j.jaccpubpol.2003.09.001
28. Varian, H. (2004). System Reliability and Free Riding. Advances in Information Security, 1–15. doi: https://doi.org/10.1007/1-4020-8090-5_1
29. Anderson, R., Moore, T. (2006). The Economics of Information Security. Science, 314 (5799), 610–613. doi: https://doi.org/10.1126/science.1130992
30. Bohme, R., Moore, T. (2009). The Iterated Weakest Link A Model of Adaptive Security Investment. In Workshop on Economics in Information Security.