Наведені результати розробки моделі поведінки антагоністичних агентів в умовах кіберконфлікта. Показано, що отримана модель може використовуватися для аналізу процесів інвестування в системах безпеки з урахуванням припущення, що на інвестиційні процеси значною мірою впливає поведінка агентів, що беруть участь в кіберконфлікті.

Представлено загальні підходи до розробки моделі. Перш за все, сформована система понять, припущень і обмежень, в рамках яких і повинна бути розроблена математична модель поведінки. З урахуванням цього розроблено математичну модель поведінки конфліктуючих агентів, яка представлена у вигляді алгебраїчних і диференціальних рівнянь. У розробленій моделі відображено як технічні характеристики системи безпеки, так і психологічні особливості учасників кіберконфлікта, які впливають на фінансові характеристики процесів інвестування систем кібербезпеки. Відмінною особливістю пропонованої моделі є одночасний розгляд поведінки сторін кіберконфлікта не як незалежних сторін, а як взаємовпливаючих один на одного агентів. Модель також дозволяє імітувати вплив що дестабілізує на поведінку конфліктуючих сторін збурень з боку середовища протистояння, змінюючи ступінь уразливості системи кібербезпеки різних векторах атак і рівень успішності їх проведення.

З використанням розробленої моделі виконано імітаційне моделювання поведінки взаємодіючих агентів в умовах кіберконфлікта. Результати моделювання показали, що навіть найпростіші стратегії поведінки атакуючої сторони ("найслабша ланка") і сторони захисту ("чекай і дивись") дозволяють забезпечити інформаційну безпеку контуру бізнес-процесів.

Розроблену модель взаємодії атакуючого і захисника можна розглядати як інструмент моделювання процесів поведінки конфліктуючих сторін при реалізації різних сценаріїв інвестування. Результати моделювання дають можливість особам, які приймають рішення, отримувати підтримку щодо напрямів інвестування в безпеку контуру бізнес-процесів

Ключові слова: моделі поведінки, антагоністичні агенти, дерево атаки, контур бізнес-процесів

UDC 681.32:007.5
DOI: 10.15587/1729-4061.2019.175978

DEVELOPMENT OF THE MODEL OF THE ANTAGONISTIC AGENTS BEHAVIOR UNDER A CYBER CONFLICT

O. Milov
PhD, Associate Professor*
S. Yevseiev
Doctor of Technical Science, Senior Researcher*
E-mail: serhii.yevseiev@hneu.net
Y. Ivanchenko
PhD, Associate Professor
Department of Information Technology Security
National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, Ukraine, 03058
S. Milevskyi
PhD, Associate Professor*
O. Nesterov
Postgraduate student
Department of Communications and Automated Control Systems**
O. Puchkov
PhD, Professor***
A. Salii
PhD, Associate Professor, Deputy head of the institute
Aviation and Air Defense Institute **
O. Tymochko
Doctor of Technical Science, Professor
Department of air navigation and combat control of aviation
Ivan Kozheduba Kharkov National Air Force University
Sumskaya str., 77/79, Kharkiv, Ukraine, 61023
V. Tiurin
PhD, Associate Professor, Head of the institute
Aviation and Air Defense Institute**
A. Yarovyi
Head of Education Department***
*Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Nauki ave., 9-A, Kharkiv, Ukraine, 61166
**National Defense University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotsky ave., 28, Kyiv, Ukraine, 03049
***Institute of Special Communication and Information Protection National
Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Verhniokluchova str., 4, Kyiv, Ukraine, 03056

Received date 13.05.2019
Accepted date 26.07.2019
Published date 28.08.2019

1. Introduction

The Internet revolution has radically changed the way people, companies and governments communicate and conduct business. But at the same time, this global interconnectedness increased the vulnerability of computer systems to information security breaches. Protection of information systems, data, intellectual property and business processes from attacks, misuse or technical failures has become and, according to forecasts, will remain a key task for organizations.

Studies related to the economics of information security [1–3], that is, the question of how much to spend on security countermeasures, despite their large number, demonstrate the following features.

First, most of them are purely economic in nature, that is, the discussion of investment issues in the cybersecurity system is conducted exclusively using financial categories such as investment portfolio, profitability, payback period, discounted profit, etc. [4–6]. That is, purely economic analysis methods are used to describe and analyze systems that, by their nature, are more organizational and technological.

Second, the findings of the researchers do not always coincide, and often they are just the opposite. This can be explained by the fact that investment in information security does not usually bring direct cash benefits, such as higher incomes or lower costs; their main contribution is to prevent possible economic losses [7, 8]. Again, this can be viewed as a discrepancy between the methods used and the features of the objects being analyzed.

Most of the publications consider the protection object as a kind of "black box", to which various cyber attacks are directed, the effectiveness of opposing to which depends on the amount of funds invested in security. At the same time, no comments are made on where exactly the invested funds are directed. In other words, the structure of the protected object in terms of both executable operations and the resources required for this is not done. At the same time, there is practically no mention in the publications about the level of protection provided, tacitly assuming that the higher the better [9, 10].

The data and systems protection efforts carried out by practitioners and scientists focused primarily on the technical aspects of cybersecurity, that is, which assets need protection at a certain level and which security countermeasures provide this protection. Taking into account the high cost of cybersecurity measures and budget constraints, a "fully protected organization" is not only a difficult, but also unattainable goal [11–13]. Instead of total protection of the organization, the organization's business processes should be considered, on which the financial well-being of the organization depends, which can be viewed as the goal of the organization's functioning. This view reflects a service-oriented approach that defines important services and service packages in an organization. Threats and vulnerabilities are assessed in the context of services, and not for individual assets. Because the organization has fewer services than assets, analysis takes less time and is better managed than assets. A service-oriented perspective is better connected with generating business revenue [14].

Business objectives and processes to support and achieve goals are in the focus of business risk assessment. The idea is to identify and analyze business processes and assign them value according to how they are related to business goals. To do this, vulnerabilities and threats for these processes are identified and assessed. The impact of accessibility, integrity and confidentiality violation on critical business processes, as well as information systems that support these processes, the valuation of which is directly related to business revenues, is evaluated [15, 16].

There are several advantages in terms of business. Since this structure is based on the classic of business management – Michael E. Porter's value chain model, it is much more comprehensible for the top management of the organization than the traditional model focused on assets-threat-vulnerability. The approach is efficient in terms of time, costs and resources, since a detailed analysis of assets, possible threats and vulnerabilities is not required. The main directions are set by important business processes. The approach also supports business process reengineering and business continuity planning, which would otherwise be performed as a separate analysis [17].

Thus, the loops of the organization's business processes and security business processes should be the objects of protection.

The loop of the organization's business processes is a set of information resources and related business processes, the fulfillment of which in a given sequence leads to the achievement of the organization's goal:

$$S^{BC} = \left\{ \left\langle S^{BP_1}, IR^{BP_1}, T^{BP_1} \right\rangle, ..., \left\langle S^{BP_n}, IR^{BP_n}, T^{BP_n} \right\rangle \right\}.$$

The security system business process loop is a set of business processes and the resources necessary for them, the implementation of which ensures the normal functioning of the organization's business process loop:

$$S^{SC} = \left\{ \left\langle S^{BP_1}, Rs^{BP_1}, T^{BP_1} \right\rangle, ..., \left\langle S^{BP_m}, Rs^{BP_m}, T^{BP_m} \right\rangle \right\}.$$

The practice of cyber defense of business processes has demonstrated the following feature. The effectiveness of cyber defense of business process loops depends on the amount of investment that is directed to the respective areas. At the same time, decisions on the allocation of certain amounts fall within the "wait and see" scenario, i. e. decisions are of reactive nature and are taken upon the implementation of a successful cyber attack. On the other hand, the attacking side acts according to the "weakest link" scenario. 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 seen as confirming the relevance of developing behavioral patterns for the interacting parties of the cyber conflict.

2. Literature review and problem statement

Taking into account the remark made at the end of the previous section, it should be noted that the investment model of security systems should reflect, first of all, the behavioral characteristics of the participants in a cyber conflict.

The most frequently cited model of investing in information security is a single-period model [3, 4], which determines the optimal amount of investment to protect information and information systems. According to the Gordon-Loeb (GL) model, the optimal level of investment is achieved when the marginal utility of investment equals the marginal cost of investment. The proposed theoretical economic GL model has demonstrated that for the given functions of the probability of violation of the protection perimeter, the maximum amount that a risk-neutral company should invest in information security does not exceed 37 % of its expected losses due to security breaches. The authors of the GL model also state that firms with limited financial resources should focus on protecting information with medium-level vulnerabilities, since protecting extremely sensitive information can be extremely expensive. Later, a modified Gordon-Loeb model [9] was proposed by expanding the

scope of the GL model, incorporating external effects and showing that socially optimal investments in information security increase by no more than 37 % of the expected loss.

It should be noted that the GL model is primarily a theoretical framework that helps security professionals understand the economics behind investing in information security. The authors of the GL model provided an illustrative example [10], demonstrating the definition of the appropriate level of investment in information security in the real case. However, the actual limitations in the practical implementation of the model are much more stringent.

Another limitation is related to the simplification of the model, according to which investments are directed to protecting the sole information resource of the organization. In fact, investments can be made to protect various information resources, as there are correlated risks in the system and modern practical solutions are often multifunctional. The third flaw questioned the suitability of the selected function families in the GL model. In [18, 19], it is argued that there is no reason to assume that the functions used reflect any real scenario for reducing vulnerability.

The GL model assumes the use of it by a risk-neutral decision maker (DM). In [20], optimal investment in security is determined in case a decision is made by a non-risk-minded decision-maker. In addition, the optimal level of investment depends on the asset to be protected, the vulnerability of the asset and the potential loss associated with it. The model also simulates one attack of a single attacker for one period with a fixed potential loss, which is an excessive simplification of reality. Compared to the risk-neutral GL model, a non-risk-minded decision maker increases his investment while increasing the expected loss, but no more than the amount of the loss. Under these conditions, there is a minimum potential loss, below which the optimal investment is zero.

In [2], the optimal level of investment in security is investigated under various attack scenarios – in the case of targeted and opportunistic attacks. When there are no budget constraints, total investment falls when a particular vulnerability reaches a certain level. There is also a minimum level of vulnerability, below which investments are zero. When the total budget is limited, investments in protection against a certain type of attack increase, when potential losses from an attack increase, or when the budget size increases. The results of the analysis show that a limited budget is allocated to mitigate the vulnerabilities that cause the most damage, and which are often associated with targeted attacks, with the result that organizations with very limited security budgets are subject to opportunistic attacks. The same results with a similar approach based on the GL model were presented in [21].

The GL model [3, 10], the modified GL model [9] and the studies [2, 20–22] can be considered as theoretical foundations that provide good economic rationales for cybersecurity investment decisions regarding the optimal level of investment and budget allocation to eliminate certain vulnerabilities. However, the simplifying assumptions are too broad to use these approaches in practice, regardless of the size of the firm that plans the investment. An information resource used by a business process is rarely exposed to a single threat or attacked by a single attacker. Investment decisions in these approaches are made on the basis of a combination of vulnerability and size of loss, which is treated as permanent. Models operate with a single variable in the risk equation, namely, with decreasing overall vulnerability, to reduce the likelihood of attacks that cause the most damage. In fact, the risk equation can be solved by taking the level of exposure instead or using a combination of detection, preventive or corrective measures.

Another analytical model [23], which considers the optimal level of investment in information security, has more realistic assumptions, such as the presence of various simultaneous attacks, and the model's goal is to analyze the distribution of investments in relation to targeted and opportunistic attacks.

Even if we exclude the theoretical nature of the models analyzed above and assume that they can be used in practice, the approaches are not universal, equally acceptable for different business structures. The considered models are more focused on large firms with a deep hierarchy of management. The upper level determines the amount of finance that can be used to ensure information security, and the next levels in the organization choose measures in accordance with the budget constraint. A small firm has a single budget that includes all of its investments and expenses. Each investment in information security must compete for limited financial resources with other investments. The models that optimize the information security budget are aimed primarily at large companies with complex business processes.

The "analytic hierarchy process" (AHP) is a universal mathematical method for making multi-criteria decisions, including both quantitative and qualitative criteria, as well as expert assessments. In [24], instead of constructing a mathematical investment model, it was proposed to consider the investment process as a multi-criteria task. To solve it, it is necessary to define many goals, set their priority and importance for decision-makers, to form a set of quantitative and qualitative indicators of achieving goals. The rules of comparison (preference) of their values, presented both in quantitative and qualitative terms, should also be specified. The AHP approach is used not only to evaluate alternatives to investing in information security in order to make the most effective use of a limited security budget, but also to justify additional investments in security, if possible. The authors propose to use the evaluation option of the AHP, forming criteria and subcriteria for the distribution of investment budget funds, as well as determining the weights of these criteria. Each alternative to maintain and improve security is evaluated for each criterion and subcriterion separately, and then receives an assessment that reflects how well the alternative distribution of the invested funds meets a certain criterion or subcriterion. The proposed criteria are: confidentiality, data integrity, and availability. The latter can be divided into three subcriteria: authentication, reliability and availability. Each criterion and subcriterion may have different importance. The following importance estimates were proposed in [24]: exceptionally high, extremely high, very high, high, fairly high, and moderately high. This rating scale allows you to correctly justify decisions made in the absence of quantitative assessments, replacing them with appropriate qualitative expert assessments.

The AHP methodology requires careful preliminary preparation – a clear definition of the criteria, sub-criteria and obtaining their comparative assessments. It is necessary to determine the essence of the criteria importance, which are subjective in nature and can be interpreted differently by decision-makers. It is often difficult to establish boundaries between the importance of criteria. For example, grades:

exceptionally high, extremely high, very high, high, fairly high, and moderately high have very close meanings. Even if the importance of the criteria is well defined, the nature of uncertainty in the case of information security risks can make the assessment problematic. Using the AHP to evaluate information security investment alternatives requires good security expertise and a thorough understanding of the methodology. The described methods can be implemented in the behavior models of interacting agents of cybersecurity systems in the case of a significant variety of implemented attacks and means of counteracting them. However, real statistics of cyberattacks committed, even in relation to critical infrastructure facilities, show that the variety of attacks, as well as countermeasures, is insignificant. The variety and intensity of threats depend, first of all, on the capabilities of the attacker (the power of his computing facilities), secondly, on the goals and objectives of the attacker, and thirdly, on the "price" of confidential information.

In [25], a class of business structures is pointed out for which the AHP approach may be acceptable, as well as difficulties associated with its preparation and use are noted. The approach can be used by small firms to evaluate investment alternatives if they have clear security objectives, which is doubtful. At the same time, there is a need to search for security experts as consultants who have knowledge and experience of working with the model, while working closely with the CEO of the company to decide on the criteria, sub-criteria and their importance for the company. This is a time-consuming process, and the economic justification for using this approach is doubtful, since the analysis itself may be more expensive than the solution necessary to ensure security.

[26] demonstrated the possibility of combining the AHP method with linear programming to select alternative options for investing in information security. Despite a rather unexpected combination of decision support methods, the main direction of the methods used is optimization of the investment project portfolio in the field of information technology (IT) security in the organization. The motivation for using the proposed approach is extremely conflicting and changing requirements for the cybersecurity of organizations, in addition to the variety of initial conditions encountered in organizations. The peculiarity of using the proposed combination of methods is as follows. Instead of ranking or evaluating various alternatives based solely on their advantages, by defining the goals of the organization and then coordinating the decisions with the goals, it is possible to optimally allocate resources for all projects in the investment portfolio. The approach described in this article is to provide a general decision-making structure that can be adapted by practitioners and adjusted by other researchers. The proposed approach may be of interest in modeling the behavior of a group of decision-makers with their own preferences, with subsequent coordination of decisions and preferences.

In [27], an optimization model is presented that combines the cost of selected security measures and the level of confidence in achieving security goals. Discrete dynamic programming was used to obtain a Pareto optimality compromise curve containing alternative security solutions. Budget constraint dictates the best security solution available on a crooked compromise. According to [28], the proposed method is limited and does not allow finding equivalent security alternatives with the same confidence level. In [28], an evolutionary optimization algorithm is used to determine equivalent safety profiles at the same cost level.

The disadvantage of both models is the lack of consideration of the measures interaction in the security profile. The security measures in the profile, apparently, are aggregated mechanically, without taking into account the overall effectiveness. In other words, these methods are not applicable in the context of synergistic threats. In general, the methods may be applicable in large firms to agree on alternative sets of security measures. At the same time, the methods require a deep understanding of the organization's security goals and the necessary actions and resources to achieve the goals. The interconnection of security goals and business goals (that is, the interaction of the loops of business processes and security processes) is not provided by the mentioned methods.

In [29], the dilemma of the system administrator is solved, that is, security measures are selected within the budget constraint and at the same time, residual damage is minimized. The paper considers the security problem as a series of successive attacks by an attacker to achieve his goal. The attacker is looking for vulnerabilities that can be used to penetrate the system to find new vulnerabilities in the system for further development. It is also assumed that the attacker can bypass the defense at a certain cost. The authors argue that the decision to manage security should take into account the possible benefits of the attacker. The attacker is not motivated to attack if the effort exceeds the gain. At the same time, the authors argue that the goal of the attacker can only be damage, so the benefit does not have to be a monetary gain. An attack tree is used to model the dynamic interaction between the attacker and the defender. Multipurpose optimization and competitive co-evolution were chosen to conduct a cost-benefit analysis. The authors emphasize the importance of a long-term security policy and that countermeasures should not be based on cost-benefit calculations of intermediate strategies.

The attacker's description, motivation, and actions indicate that this approach is more suitable for analyzing targeted than random attacks. This computationally complex approach is based on game theory methods, which puts forward certain requirements for both the design of models and their further use. Despite its complexity, the described model is too simplified to cover the cost aspects of security measures. The model assumes that security measures are independent of each other, which is not a practical assumption. Security effectiveness can be achieved when the selected set of security measures takes into account interdependencies. The authors define security measures as preventive measures to stop an attacker who has reached his goal. The focus is on the costs and benefits of the attacker. The model does not clearly take into account the choice of recovery measures in order to reduce the costs that arise in the event of attacks. In some cases, it may be appropriate not to invest in the prevention of attacks, but to invest in minimizing the costs arising from attacks. By its nature, this model is perhaps the most consistent with the tasks of constructing models of the behavior of interacting agents under conditions of cyber conflict.

The work [30] considers the problem of investments in information security related to cash costs of implementation, indirect costs and risk reduction. The paper introduces a distinction between "passive" and "active" threats. The former represent attacks independent of defense, the latter show the attacker's ability to respond to implement-

ed defense. The peculiarity of the work is that it considers multistage attacks and potential correlations in successful actions at various stages. The combined effectiveness of countermeasures is determined by choosing the effectiveness that is the highest among them. The paper uses nonlinear multipurpose integer programming and mixed transforms of integer and linear programming to find Pareto optimal solutions.

In [31], a methodology is presented for finding the optimal combination of security measures within a given budget. The first step is to analyze risks and evaluate the effectiveness of countermeasures against various vulnerabilities. Based on the results of the risk assessment, control games between the defender and the attacker are simulated using various vulnerabilities. Multipurpose multiple-choice knapsack optimization techniques are used in the solutions of various control games in order to decide on the distribution of the security budget. In [32], stochastic programming is used to make investment decisions on various types of countermeasures within a given budget. In addition to the security competency required to use the approaches, experience in mathematical modeling is also required. The models presented above deal with the problem of finding the best set of countermeasures that maximize security within limited financial resources.

The work [33], devoted to the choice of security measures, uses the attack tree approach to analyze information security risks and assess the cost and probability of success of attacks from the attacker's point of view. The authors consider rational profit-oriented attackers who compare their success and benefits with the cost of carrying out the attack and possible fines if they are captured and punished. A rational attacker is unlikely to attack if the expected costs exceed the benefits. The paper suggests a simple method of economic justification of security measures – the search for an adequate set of measures sufficient from a security point of view. Sufficiency in the context of the proposed model means the minimum probability of an attack, which is considered as the main one. Adequacy implies that the cost of protective measures should not exceed the value of the assets to be protected.

The model takes into account two players – the attacker, who is aimed at a specific organization. In fact, an attacker can have several goals. A rational attacker will attack the company where he expects the greatest benefit. Thus, any security measure that makes an attack more costly for an attacker can prevent the attack. The formulation of the sufficiency condition established in the model, which may turn out to be economically irrational, is also doubtful. The ultimate goal of a rationally acting company is not to prevent attacks, but to minimize the risk of them. It may be more costly for a company to prevent an attack than to invest in security measures that minimize the impact of the attack. Therefore, the sufficiency condition in this model can lead to excessive investment in security.

The use of game theory methods to assess not only investment volumes, but also their effective distribution by objects that differ in the amount of information, vulnerability, and probability of attack, is given in [34]. The authors of the work rightly note that the search for a solution is complicated by the uncertainty of the opponent's actions. Under these conditions, a satisfactory solution is proposed that corresponds to the saddle point of the objective function. This function can express one of the indicators of the defense system – the share of lost information, profit from investments in defense, their profitability – depending on the ratio of attack and defense resources, accordingly. The paper analyzes the conditions for the existence of a saddle point in one- and two-level systems, which differ in the number of objects and obstacles that protect them. The intervals of the ratios of the means of the attacking and the defending sides are found in which a saddle point can exist. It is shown that the saddle point existence intervals are determined by the form of dynamic vulnerability of objects and the distribution of information among objects. However, it should be noted that the application of this approach encounters certain difficulties in practical implementation. First of all, all strategies for the behavior of opponents should be known, which allows you to build a complete game matrix. Cost estimates of player behavior strategies should also be known. At the same time, the construction of the objective function may turn out to be an ambiguous process due to the incomplete awareness of the player about the possible response actions of the enemy. All these requirements for the mathematical formulation of the problem can make the application of game theory methods extremely difficult and sometimes impossible [35, 36].

In [37], an approach is presented related to the application of game theory for predicting the behavior of players, as well as designing mechanisms for the interaction of agents with directly opposite goals. Attention should also be paid to the presented explanation of how a large number of people with different interests interact (the so-called non-coalition or non-cooperative games) in modern global technical systems, such as the Internet. In particular, the explanation of how in such systems the common good is often achievable without the intervention of a single governing body ("dictator") is noteworthy.

In [38], an approach to the construction of a cyber world is proposed, which is designed to study the security of cyber systems operating on the Internet. These systems are represented as a complex of various interacting teams of intelligent agents. This work differs from other similar ones in that it considers various options for the interaction of team agents, which can be both in a state of antagonistic confrontation and cooperation. The task of analyzing interacting agents is considered as an example of distributed denial of service attacks. The environment was implemented on the basis of a discrete event modeling system, which made it possible to integrate agent-based modeling with simulation of basic Internet protocols. Despite the technical elaboration of approaches to modeling agent behavior, issues of assessing the economic efficiency of interaction or opposition are not considered in the work. However, it can be considered as the foundation on which the "building" of economic assessments of the effectiveness of the strategies used for the behavior of interacting agents can be built.

An example of the practical application of the behavior models of interacting agents under conditions of cyber conflict is given in [39]. A search model for rational options for strategies for mutual investment management in the cybersecurity systems of large educational institutions is considered. The work demonstrates various relationships between the parameters of investing in cybersecurity systems and solving other problems related to the protection of the information and educational environment of large educational institutions. The developed model is recommended

primarily as an information-algorithmic component for a decision support system for the analysis and optimization of mutual investment strategies in the information and educational environment of educational institutions and their cybersecurity systems. The difference between the proposed solution and similar in this segment of scientific research is the ability to determine specific parameters and recommendations in the process of mutual investment. Reference should be made to the work [40], in which the issues of cyber defense of educational resources are brought up to the level of development of a classifier for cyber threats, which allows to give cost estimates of both information resources and the costs of attacks and means of counteracting them.

Studies related to the economics of information security, that is, the question of how much you need to spend on security countermeasures, despite their multiplicity, demonstrate the following features. Firstly, most of them are purely economic in nature, that is, the discussion of investment issues in the cybersecurity system is conducted exclusively using financial categories, such as investment portfolio, profitability, payback period, discounted profit, etc. That is, methods of analysis of purely economic systems are used to describe and analyze systems that, by their nature, are more socio-technological.

Secondly, the findings of the researchers do not always coincide, and often they are just the opposite. This can be explained by the fact that investment in information security does not usually bring direct cash benefits, such as higher incomes or lower costs; their main contribution is to prevent possible economic losses. Again, this can be viewed as a discrepancy between the methods used and the features of the objects being analyzed.

In most publications, the object of protection is considered as a kind of "black box", to which various cyber attacks are directed, the repel efficiency of which depends on the amount of funds invested in security. At the same time, no comments are made on where exactly the invested funds are directed. In other words, the structure of the protected object in terms of both executable operations and the resources required for this is not done. However, there is practically no mention in the publications about the level of protection provided, tacitly assuming that the higher the better.

3. The aim and objectives of the study

The aim of the study is to develop a model of the behavior of antagonistic agents under a cyber conflict, the purpose of which is the possibility of scenario modeling of the behavior of the parties to cyber conflict, ultimately influencing the choice of the direction of investing limited financial resources of the investment budget.

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

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

– to develop the mathematical model of interaction between the parties to the conflict, influencing the adoption or change of previously made investment decisions;

– to perform simulation modeling based on the developed mathematical model to confirm the logic of the behavior of the parties to the conflict and assess the impact of their behavior on the use of investments.

4. Basic concepts in models of interaction between the parties under a cyber conflict

The analysis carried out in [41] made it possible to formulate a list of basic concepts and categories used in the description of investment processes in security systems that should be used in the developed model of antagonistic agents behavior. Table 1 presents the basic concepts related to investment strategies in cybersecurity systems that underlie the interaction of the defender and the attacker in a dynamic behavior model.

Table 1

Basic concepts in the models of interaction of the cyber conflict parties

Concept	Definition
Reputation	Favorable and universally recognized name or reputation for merits, achievements, reliability, etc. In this case, the reputation refers to the public authority of the company
Vulnerability	The level of security possessed by company assets. It can also be called the asset protection level
Security Vectors	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 set 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
Defender Opportunities	Available resources are distributed among assets to increase the level of asset sustainability
Attackers Opportunities	Part of the resources of attackers available for distribution among the defender's assets
Share of investment	Part of the opportunities aimed at protecting the company's assets
Share of attacks	The number of attacks that cybercriminals distribute between the security vectors of defenders in accordance with previous successful attacks
Successful attacks	Attacks capable to violate asset protection through security vectors
Profit of Defenders	Monetary benefit from improving asset security, which in turn enhances reputation, thereby improving financial performance
Attackers Welfare	Monetary advantage from violation of defenders' assets
"WeakLink" Investment Strategy	The weak link strategy is that the attacker rationally puts more effort into attacking systems with a low level of security. Once the organization's perimeter is broken, attackers can often take advantage of this
"Wait and See" Investment Strategy	The basic idea is that in case of uncertainty about the expected benefits, it may be better to wait for key events. Once a security breach occurs, more information appears to evaluate the expected benefits of security investment, which makes the assessment more accurate

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.

The model was based on the assumptions and limitations presented in Fig. 1.

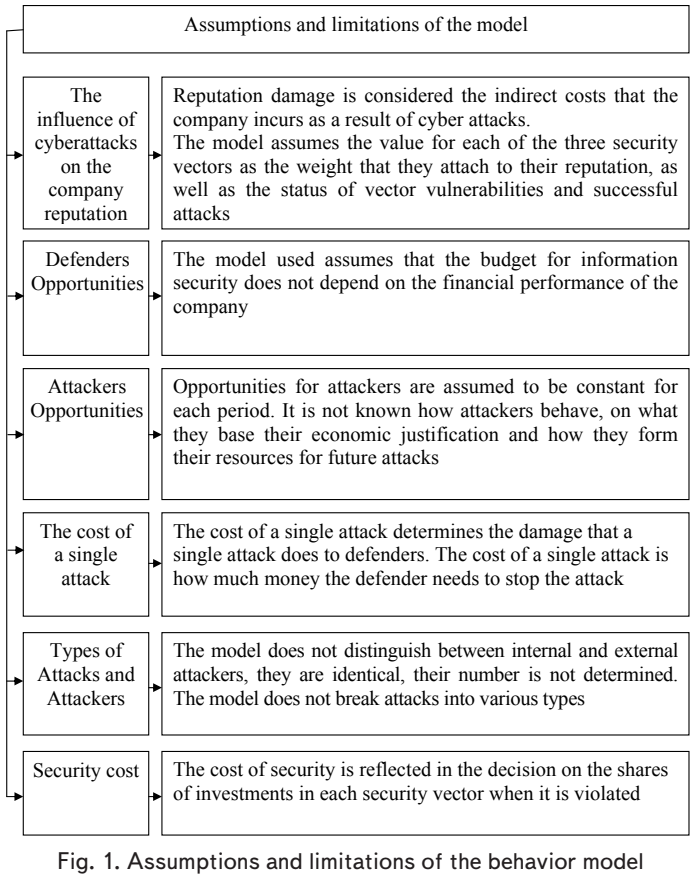

Fig. 1. Assumptions and limitations of the behavior model

The following should be indicated as the main limitations of the developed model. The model is limited to only three threat vectors and means to counter them. Such a restriction from the point of view of the practical implementation of the model is reasonable, based on the variety of attacks carried out on a particular object. It is also not critical, since the proposed model can be easily adapted not only for a specific type of cyberattack, but also for their number.

The second limitation of the model is the unified cost of cyber attacks for all vectors, and independent of countermeasures. This limitation can also be easily removed in the process of adapting the model for a particular cyber attack object and type.

The model also does not include various financial indicators and approaches for analyzing each investment decision, such as: cost-benefit analysis, risk analysis, net present value (NPV), annual loss expectancy (ALE), return on security investment (ROSI), and others. The reason for this is that financial analysis would require a more complex model, including empirical data, to give greater accuracy to the results of the study. These issues can be considered as directions for future research.

5. Development of a mathematical model of the behavior of the parties to cyber conflict

The model focuses on the dynamics of the interaction of the attacker and the defender in the field of information security in order to discover the investment strategies used by opponents.

The model represents a defender who protects assets from a group of cybercriminals trying to compromise a company's assets with 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.

The formation of the model is limited by three possible threats, which can be considered as separate security vectors of access to the company's information assets. Each information asset can be protected by investing in appropriate protection. For each security vector, there is one access method and one protection method. Finally, protection is effective if it can repel incoming attacks.

The model consists of three submodels, which are shown in Fig. 2: defender submodels, confrontation environment submodels, and attacker submodels.

The Defender's model represents a defense mechanism against cyber attacks aimed at violating the security of an information asset. In each period, the defender makes a decision on choosing the target investment information resource to determine his own protection configuration. It is assumed that the defenders have basic protection for each vector, and their capabilities are sufficient for additional efforts undertaken in case of security breaches.

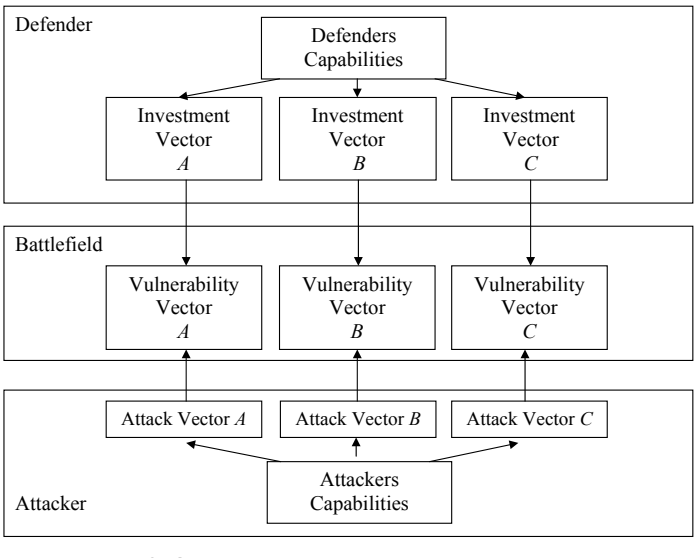

Fig. 2. General structure of the interaction model

The defender organizes the protection of his own information assets with the help of countermeasures displayed by three security vectors (A, B and C). The result of the defense, ultimately, affects the reputation of the company,

which can be measured by financial results. In the model, security vectors are described by the vulnerability state of each vector. At the end of the attack, information about its success or reflection (indicating a specific security vector) becomes available. For each of the vectors, successful and repulsed attacks are counted. The share of investments for each security vector is calculated based on the share of successful attacks on this vector in the total number of successful attacks. This means that the defender will invest the appropriate share of investments in the corresponding security vector, which is proportional to the number of successful attacks conducted against this vector.

Reputation is measured in relative units. Reputation is adjusted based on the results of successful or repulsed attacks across all security vectors. In the case of repulsed attacks, the reputation of the company increases, while successful attacks result in a loss of reputation.

The financial indicators of the defenders are determined on the basis of expert estimates of the monetary value of each reputation score.

The attacker is aimed at violating the security of the company's business processes and makes some efforts to attack. Since the attacker does not know exactly what resources his attack should be directed to, for gaining profit he bases his actions on the knowledge of the successful attacks distribution on target resources known to him from previous experience.

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 correspond to lower financial indicators for the defender. The attacker does not act indiscriminately; he rather attacks only when it is beneficial.

Successful historical attacks in the attacker's model prompt him to direct attacks to the weakest link, not neglecting the other objectives of the attack, but allocating a smaller part of the resources for their attack.

The sum of the accumulated successful attacks for each vector allows the attacker to determine the weakest link and make a decision for the next attack in order to use the most vulnerable security vector.

The distribution of the attack direction is determined by the attackers as a result of the accumulated successful attacks for each vector. To implement the strategy of the weakest link in this model, attackers must switch from one direction of attack to another when the current direction is not favorable for him to continue attacks.

To make a decision on changing the attack vector, it is necessary to compare the current value of accumulated successful attacks with the same value for the previous period. To do this, the "switch" parameter is used, which indicates that when the ratio of the current value to the value of the previous period is less than 1, it is not profitable for the attacker to continue using this vector and it is necessary to proceed to attacks in other directions.

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

The effectiveness of attackers is the sum of violations of all vectors multiplied by the cost of a single attack. The welfare of attackers is determined by financial indicators, the increase of which is a function of the productivity of attackers.

To reflect the interaction of defenders and intruders, each of which has certain capabilities and make appropriate investment decisions, a third model is implemented – a model of the confrontation environment (battlefield). The main variables of this model are vulnerability and successful attacks on each security vector.

Vulnerability means the security level of each of the attack vectors. The positive value of the vulnerability indicates the weaknesses in ensuring security in this area of protection. This indicator can be calculated based on the ratio of defender and attacker investments in this area of defense and attack.

In essence, the vulnerability is determined by the difference between the resources that the attacker directs to the corresponding vector and the resources that the defender allocates to fix security flaws in the same vector.

Successful attacks are important for this model, as they will initiate subsequent investment decisions for both opponents. So 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 repel all attacks. On the other hand, if the vulnerability of the vector is above zero, successful attacks should be expected. The share of invested funds to protect a given direction in combination with the cost of repelling an attack in this direction determines the number of attacks that a defender can repel in case of a security breach.

The constants used in the model, which are set at the beginning of the simulation and allow modeling various scenarios of the interaction of antagonistic agents and the distribution of investments following from this, are presented in Table 2.

Table 2

Parameters of the behavior model of the interacting parties to the conflict

Symbol	Description
c_1	Number of Dismissed Attacks
c_2	Activated Uncertainty
c_3	Attackers Capabilities
c_4	Attack Unitary Cost
c_5	Base financial performance
c_6	Base reputation
c_7	Defenders Capabilities
c_8	Dismissal time
c_9	Information Sharing
c_{10}	Reputation to money rate
c_{11}	Time of reputation loss
c_{12}	Time to build up reputation
c_{13}	Time to report attack
c_{14}	Vector A Value
c_{15}	Vector B Value
c_{16}	Vector C Value

The designations of the variables used in the model are presented in Table 3.

Table 3

Variables of the behavior model of the interacting parties to the conflict

Symbol	Description	Symbol	Description
x_1	Reputation	x_{25}	Vulnerability of Vector B
x_2	Reported Reputation	x_{26}	Vulnerability of Vector C
x_3	Adjustment	x_{27}	Successful Attacks on Vector A
x_4	Dismissed A	x_{28}	Successful Attacks on Vector B
x_5	Dismissed B	x_{29}	Successful Attacks on Vector C
x_6	Dismissed C	x_{30}	Breaches Vector A
x_7	Defenders Financial Performance	x_{31}	Breaches Vector B
x_8	Fraction of Attacks on Vector A	x_{32}	Breaches Vector C
x_9	Fraction of Attacks on Vector B	x_{33}	Accumulated Successful Attacks on Vector A
x_{10}	Fraction of Attacks on Vector C	x_{34}	Accumulated Successful Attacks on Vector B
x_{11}	Report on Vector A	x_{35}	Accumulated Successful Attacks on Vector C
x_{12}	Report on Vector B	x_{36}	Past Value A
x_{13}	Report on Vector C	x_{37}	Past Value B
x_{14}	Reported Successful Attacks on A	x_{38}	Past Value C
x_{15}	Reported Successful Attacks on B	x_{39}	Switch A
x_{16}	Reported Successful Attacks on C	x_{40}	Switch B
x_{17}	Fraction of Investment in Vector A	x_{41}	Switch C
x_{18}	Fraction of Investment in Vector B	x_{42}	Attackers performance
x_{19}	Fraction of Investment in Vector C	x_{43}	Accumulated Attackers Wealth
x_{20}	High Uncertainty	x_{44}	Defenders Accumulated Profits
x_{21}	Low Uncertainty	x_{45}	Adjustment
x_{22}	Middle Uncertainty	x_{46}	Erosion
x_{23}	Uncertainty	x_{47}	Accumulated Attackers Wealth
x_{24}	Vulnerability of Vector A	x_{48}	Increasing Financial Performance

A formal presentation of the basic relationships between the variables described earlier and determining the essence of the relationship between the participants in the cyber conflict, leading to a change in the investment scenario and the redistribution of funds, is given below in the form of an algebraic and differential equation system. Taking into account the presence of feedback in the real interaction of the parties of the cyber conflict (reinforcing and damping circuits), the moment of time should be indicated for each variable, however, such a record significantly cluttered the system of equations.

$$dx_1/dt=x_{45}-x_{46},$$

$$x_2=c_6-(c_{14}\times x_{24})-(c_{15}\times x_{25})-(c_{16}\times x_{26}),$$

$$x_3=x_2-x_1,$$

$$x_4=c_1/c_8,$$

$$x_5=c_1/c_8,$$

$$x_6=c_1/c_8,$$

$$x_7=(c_{10}\times x_1)+c_5,$$

$$x_8=x_{39}\times x_{33}/(x_{33}+x_{40}\times x_{34}+x_{41}\times x_{35}),$$

$$x_9=x_{40}\times x_{34}/(x_{39}\times x_{33}+x_{34}+x_{41}\times x_{35}),$$

$$x_{10}=x_{41}\times x_{35}/(x_{39}\times x_{33}+x_{40}\times x_{34}+x_{35}),$$

$$x_{11}=x_{27}/c_{13},$$

$$x_{12}=x_{28}/c_{13},$$

$$x_{13}=x_{29}/c_{13},$$

$$dx_{14}/dt=x_{11}-x_4,$$

$$dx_{15}/dt=x_{12}-x_5,$$

$$dx_{16}/dt=x_{13}-x_6,$$

$$x_{17}=x_{14}/(x_{14}+x_{15}+x_{16}),$$

$$x_{18}=x_{15}/(x_{14}+x_{15}+x_{16}),$$

$$x_{19}=x_{16}/(x_{14}+x_{15}+x_{16}),$$

$$x_{20}=c_9\times\text{rnd}(\min((0.75+0.00498\times t),0.999),\ \max(1.5-(0.00998)\times t,\ 1.001))+(1-c_9)\times\text{rnd}0.75,1.5),$$

$$x_{21}=c_9\times\text{rnd}(\min((0.95+0.0008\times t),0.999),\ \max(1.1-(0.0018)\times t,\ 1.001))+(1-c_9)\times\text{rnd}\ (0.95,1.1),$$

$$x_{22}=c_9\times\text{rnd}(\min((0.875+0.00248\times t),0.999),\ \max(1.25-(0.00498)\times t,\ 1.001))+(1-c_9)\times\ \times\text{rnd}\ (0.875,1.25),$$

$$x_{23}=\text{if}(c_2=0,1,\ \text{if}(c_2=2,x_{22},\ \text{if}(c_2=1,\ x_{21},\ x_{20}))),$$

$$x_{24}=(c_3\times x_8\times c_4\times x_{23})-(c_7\times x_{17}),$$

$$x_{25}=(c_3\times x_9\times c_4\times x_{23})-(c_7\times x_{18}),$$

$$x_{26}=(c_3\times x_{10}\times c_4\times x_{23})-(c_7\times x_{19}),$$

$$x_{27}=\text{if}(x_{24}>0,\ ((c_3\times x_8)-((c_7\times x_{17})/c_4)),\ 0),$$

$$x_{28}=\text{if}(x_{25}>0,\ ((c_3\times x_9)-((c_7\times x_{18})/c_4)),\ 0),$$

$$x_{29}=\text{if}(x_{26}>0,\ ((c_3\times x_{10})-((c_7\times x_{19})/c_4)),\ 0),$$

$$x_{30}=x_{27}/c_{13},$$

$x_{31}=x_{28}/c_{13}$,

$x_{32}=x_{29}/c_{13}$,

$dx_{33}/dt=x_{30}$,

$dx_{34}/dt=x_{31}$,

$dx_{35}/dt=x_{32}$,

$x_{36}=\text{delay}(x_{33}, 1,0)$,

$x_{37}=\text{delay}(x_{34}, 1,0)$,

$x_{38}=\text{delay}(x_{35}, 1,0)$,

$x_{39}=\text{if}(x_{33}-x_{36}<\text{l},0,1)$,

$x_{40}=\text{if}(x_{34}-x_{37}<1,0,1)$,

$x_{41}=\text{if}(x_{35}-x_{38}<\text{l},0,1)$,

$x_{42}=((x_{30})+(x_{31})+(x_{32}))\times c_4$,

$dx_{43}/dt=x_{47}$,

$dx_{44}/dt=x_{48}$,

$x_{45}=\text{if}(x_3>0, (x_3/c_{12}), 0)$,

$x_{46}=\text{if}(x_3<0, (\text{abs}(x_3/c_{11})), 0)$.

The resulting system of equations describes the behavior of the attacker and defender in the process of cyber conflict, the interaction of which determines the direction of investment in the security system of the business process loop, as well as the moments of the direction change.

6. Simulation of the interacting agents behavior

The described model of interaction between attacking and defending sides was used to simulate their behavior in various conditions from the point of view of choosing strategies for investing in a cybersecurity system. In accordance with the developed methodology for modeling the behavior of interacting agents under conditions of cyber conflict [41], the developed mathematical model was implemented in the dynamic system simulation tool PowerSim (Powersim Software AS, Norway). It should be noted that any software that supports the simulation of dynamic systems can be used as a modeling environment. Alternatively-MATLAB+Simulink, AnyLogic, etc. can be offered.

As an option, modeling of the "weakest link" mechanism was chosen. This mechanism initiates investment strategies for both attackers and advocates. It is the process of interaction between the attacking and the defending parties that allows you to determine the weakest link in their vectors in order to decide on the direction and amount of investment. The mechanism of the weakest link starts with the initial conditions, reflected in the accumulated successful attacks in the submodel of attackers.

As the initial conditions, zero conditions were chosen for financial indicators (accumulated costs of attacks and their protection). To start the model and select the initial attack vector, some initial spread in the values of the accumulated successful attacks on the considered vectors must be specified. Otherwise, the attack vector should be selected randomly (the given version of the program does not provide this).

The initial conditions for successful attacks accumulated by attackers will determine the subsequent actions for both opponents. Whenever one security vector is violated in protection, significantly exceeding the other vectors, attackers use it. For a basic launch, the initial conditions for accumulated successful attacks are presented in Table 4.

Table 4

Initial modeling conditions for the "Weakest Link" scenario

Accumulated Successful Attacks. Vector A	100
Accumulated Successful Attacks. Vector B	75
Accumulated Successful Attacks. Vector C	50

In this case, vector A is the weakest link identified by the attacker in the first period. The initial values were chosen in such a way as to visually reflect the preference that the attacker gives to one of the vectors compared to the others. However, there is a second preferred vector (vector B), showing the share of the attackers' capabilities allocated for each successful attack of the vector.

Fig. 3 shows successful attacks for all three attack vectors. An interesting feature can be noted on this graph – a change in the proportion of analyzed attack vectors that the attacker performs as soon as another weak link is detected.

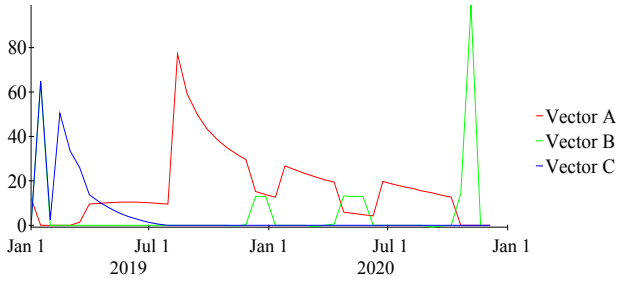

Fig. 3. Distribution of successful attacks by vectors (x_{27}, x_{28}, x_{29})

Fig. 4 shows the dynamics of the accumulation of successful vector attacks. In case of successful completion of the attack, the value of the counter of successful attacks of the corresponding vector simply increases by units.

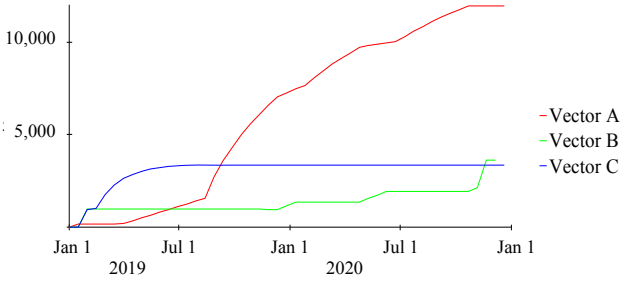

Fig. 4. Accumulation of successful vector attacks (x_{33}, x_{34}, x_{35})

Along with the change in the number of successful vector attacks, the vulnerability of the defense vectors also changes

depending on the interactions of attackers and defenders. This means that when the capabilities of attackers exceed the capabilities of defenders, the vulnerability in the protection vector that is most at risk will increase, which corresponds to a decrease in the security level of this vector. Fig. 5 shows the dynamics of the vulnerability of each security vector.

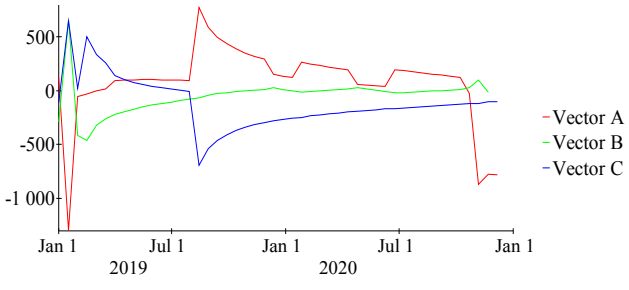

Fig. 5. Vulnerability of attack vectors (x_{24}, x_{25}, x_{26})

To better understand the dynamics of investment decisions made by both opponents when the mechanism of the weakest link is activated, Fig. 6 shows how attackers and defenders act in accordance with their respective capabilities. When an attacker determines the weakest link in the defense, he will use this advantage as long as this advantage is relevant and the defender closes the security gap, forcing the attacker to switch to another target in the following periods.

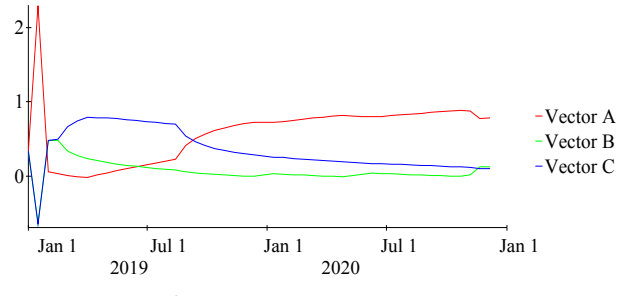

Fig. 6. Distribution of investments by attack vectors (x_8, x_9, x_{10})

Fig. 7 shows an increase in the welfare of the attackers in the base run. However, defenders can effectively protect their information assets, even if attackers successfully attack the weakest link in the security vectors.

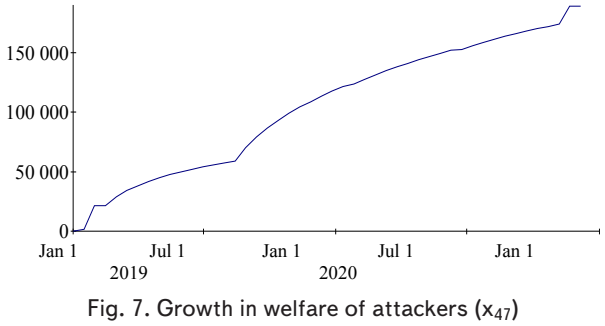

Fig. 7. Growth in welfare of attackers (x_{47})

Thus, the simulation experiment showed that attackers constantly find the weakest link and direct attacks against it (vector A). After the defender blocks attacks, the attacker switches to the next weak link.

In the case of a balance between attack vectors (equal number of successful attacks in previous periods), the application of the weakest link approach is impossible. The capabilities of attackers and defenders are the same, successful attacks do not occur, because attackers do not find the weakest link, and defenders can effectively protect their information assets.

Thus, the proposed behavior model of interacting agents in a cyber conflict has shown that even the simplest behavioral strategies of the attacking side (the "weakest link") and the defense side ("wait and see") can provide information security for the business process loop. In this case, the simulation results presented in Fig. 3–7 show that the attack side promptly switches to attacks on a different vector if the attack is successfully repelled on a previously selected vector. The defense side redirects investment resources, ensuring timely protection of the business processes, identifying the weak link in the cybersecurity system at the current time.

The obtained simulation results not only do not contradict the simulation results when using other mathematical models (both analytical and simulation) of similar processes [42, 43], but also significantly supplement the previously obtained results. This is achieved due to the fact that, unlike the ones mentioned earlier, the model operates not so much with the behavior of individual cyber conflict agents as with their joint activity, takes into account the mutual influence of agents on each other, and also takes into account the influence of the confrontation environment, which is a source of random disturbances (in particular, setting the degree of vulnerability of various attack vectors and the level of their success).

7. Discussion of the behavior simulation results of the interacting parties of cyber conflict

Analyzing the results, the following features of the relationship of the dynamics of the simulated processes should be noted.

The distribution of successful attacks by vectors (Fig. 3) is in accordance with the vulnerability of the protection vectors from these attacks (Fig. 5). This corresponds to the previously formulated assumptions inherent in the model of interaction of antagonistic agents. In particular, as soon as the vulnerability of vectors B and C becomes negative, the percentage of attacks along vector C drops to zero from the initial level of 50. This means that the business process loop security system is considered invulnerable to attacks on these vectors. After that, the attackers do not take any attacks on this vector. The reason for the fall in the vulnerability of vectors is exogenous.

The second interesting feature of the behavior of the parties to the conflict is associated with a slight decrease in the vulnerability of protection by vector A, which carries out the bulk of attacks on the business process loop. When the vulnerability drops by 15 % from the initial maximum value of 600 over a period of about 2 months, attacks are switched almost synchronously along vector B, which follows vector A in terms of vulnerability.

Fig. 4 clearly demonstrates the increase in the accumulation of successful attacks on vector B (up to 500 from the previously achieved accumulated value of 1,000, which has been preserved over the entire previous time). Moreover, by the invulnerable vector C (Fig. 5), the accumulation of successful attacks is not observed (Fig. 5), since the attacker does not consider this vector as promising for attacks.

The distribution of attacks by the corresponding vectors and their successful (or unsuccessful) conduct lead to the

next investment activity of the defending party, as follows from the definition of the "wait and see" scenario. Since no attacks are made on vector C as unpromising for the attacking side, the share of the defense investment for this vector drops to 0. Fig. 6 shows that the initial distribution of investments was set as follows: vector A – 0 %, vector B – 50 %, vector C – 50 %. Since vector A is the most vulnerable, which follows from the analysis of the attacks carried out by the defense side, the investments are redistributed between the vectors, and the share of funds allocated for protection (vulnerability reduction) from attacks of vector A increases to 80 % of the total. Since the vulnerability of the other two vectors is not zero, appropriate means are also allocated to ensure protection against attacks on these vectors (B and C). In addition, another feature of the defending side behavior should be noted. Since no attacks are undertaken with respect to vector C, the defenders cannot make a conclusion regarding the vulnerability of this vector (the absence of the results of the reflection of attacks due to their absence). Therefore, the defender does not reduce investments in vector C to zero, creating some "insurance" fund in the amount of up to 10 % of the total investment.

Fig. 7 shows a decrease in the growth rate of the general well-being of attackers, which occurs just at those times when the vulnerability of vector A falls, and, accordingly, the number of successful attacks falls. The growth rate is restored as soon as the vulnerability of vector A increases again.

The general conclusion based on the analysis of the model variables of conflicting agents interaction in a cyber conflict is the consistency of the dynamics of processes in individual stages of the security system functioning and the coincidence of the results of modeling the impact of the behavioral aspects of cyber conflict on investment processes in security systems as a whole with the results of other authors obtained on other models of the processes under consideration.

8. Conclusions

1. The basic concepts, the relationships between them and the limitations that were used in the development of the mathematical model are formed. The concepts were associated with constants and variables of the developed mathematical model. Model variables reflect both the behavioral and economic aspects of the security system functioning. These aspects together determine the nature of the participants' interaction in cyber conflict, influencing the distribution of limited investment funds. The formed assumptions and limitations of the developed model determine the degree of simplicity of the simulated processes and the resulting set of the simulated processes.

2. The mathematical model is developed that describes the interaction of defenders and attackers in a confrontation environment in the form of a system of algebraic and differential equations. The chosen form of the model representation is traditional for displaying the properties of variables and relations between them. This allows to implement the mathematical model in the form of a program model in various modeling environments at the subsequent stages of modeling (system-dynamic modeling, game-theoretic modeling).

3. The process of simulation using the software implementation of the resulting mathematical model is completed. As an option, modeling of the "weakest link" mechanism was chosen. This mechanism initiates investment strategies for both attackers and defenders. The model did not include various financial indicators and approaches for analyzing each investment decision, such as: cost-benefit analysis, risk analysis, net present value (NPV), annual loss expectancy (ALE), return on security investment (ROSI). The simulation result showed good agreement with the results obtained by other authors.

References

1. 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
2. Huang, C. D., Hu, Q., Behara, R. S. (2006). Economics of information security investment in the case of simultaneous attacks. The Fifth Workshop on the Economics of Information Security. Available at: http://weis2006.econinfosec.org/docs/15.pdf
3. Gordon, L. A., Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5 (4), 438–457. doi: https://doi.org/10.1145/581271.581274
4. Gordon, L. A., Loeb, M. P. (2006). Budgeting process for information security expenditures. Communications of the ACM, 49 (1), 121–125. doi: https://doi.org/10.1145/1107458.1107465
5. Böhme, R., Nowey, T. (2008). Economic Security Metrics. Lecture Notes in Computer Science, 176–187. doi: https://doi.org/10.1007/978-3-540-68947-8_15
6. Gordon, L. A., Loeb, M. P., Lucyshyn, W. (2003). Information security expenditures and real options: a wait-and-see approach. Computer Security Journal, 19 (2), 1–7.
7. Suby, M., Dickson, F. (2015). The 2015 (ISC)2 Global Information Security Workforce Study. A Frost & Sullivan White Paper, 46. Available at: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2015.ashx?la=en&hash=01D5BD45477FB7B45EF773366CF7D1D9BB6A6753
8. Whitman, M. E. (2003). Enemy at the gate. Communications of the ACM, 46 (8), 91–95. doi: https://doi.org/10.1145/859670.859675
9. 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
10. Gordon, L. A., Loeb, M. P., Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. Journal of Information Security, 07 (02), 49–59. doi: https://doi.org/10.4236/jis.2016.72004
11. Magic Quadrant for Security Information and Event Management. Available at: https://www.novell.com/docrep/documents/yuufbom4u2/gartner_magic_quadrant_siem_report_may2011.pdf

12. Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14–30. doi: https://doi.org/10.1016/j.cose.2015.11.001
13. Gartner IT Key Metrics Data 2012: IT Enterprise Summary Report. Available at: https://www.slideshare.net/vashistvishal/itkmd12-it-enterprisesummaryreport
14. Anderson, R. (2001). Why information security is hard - an economic perspective. Seventeenth Annual Computer Security Applications Conference. doi: https://doi.org/10.1109/acsac.2001.991552
15. Halliday, S., Badenhorst, K., von Solms, R. (1996). A business approach to effective information technology risk analysis and management. Information Management & Computer Security, 4 (1), 19–31. doi: https://doi.org/10.1108/09685229610114178
16. Khanmohammadi, K., Houmb, S. H. (2010). Business Process-Based Information Security Risk Assessment. 2010 Fourth International Conference on Network and System Security. doi: https://doi.org/10.1109/nss.2010.37
17. Yevseiev, S. (2016). Methodology for information technologies security evaluation for automated banking systems of Ukraine. Ukrainian Scientific Journal of Information Security, 22 (3), 297–309. doi: https://doi.org/10.18372/2225-5036.22.11103
18. Willemson, J. (2006). On the Gordon & Loeb model for information security investment. The Fifth Workshop on the Economics of Information Security. University of Cambridge.
19. Willemson, J. (2010). Extending the Gordon and Loeb Model for Information Security Investment. 2010 International Conference on Availability, Reliability and Security. doi: https://doi.org/10.1109/ares.2010.37
20. Derrick Huang, C., Hu, Q., Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. International Journal of Production Economics, 114 (2), 793–804. doi: https://doi.org/10.1016/j.ijpe.2008.04.002
21. Wang, Q., Zhu, J. (2016). Optimal information security investment analyses with the consideration of the benefits of investment and using evolutionary game theory. 2016 2nd International Conference on Information Management (ICIM). doi: https://doi.org/10.1109/infoman.2016.7477542
22. 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
23. Derrick Huang, C., Behara, R. S., Hu, Q. (2007). Chapter 3 Economics of Information Security Investment. Handbooks in Information Systems, 53–69. doi: https://doi.org/10.1016/s1574-0145(06)02003-4
24. Bodin, L. D., Gordon, L. A., Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. Communications of the ACM, 48 (2), 78–83. doi: https://doi.org/10.1145/1042091.1042094
25. Mamers, T. (2018). The art and science of information security investments for small enterprises. Tallinn, 109.
26. Kanungo, S. (2006). Portfolio approach to information technology security resource allocation decisions. The Tenth Pacific Asia Conference on Information Systems, 286–299.
27. Ojamaa, A., Tyugu, E., Kivimaa, J. (2008). Pareto-optimal situaton analysis for selection of security measures. MILCOM 2008 - 2008 IEEE Military Communications Conference. doi: https://doi.org/10.1109/milcom.2008.4753520
28. Kirt, T., Kivimaa, J. (2010). Optimizing IT Security costs by evolutionary algorithms. Conference on Cyber Conflict Proceedings. Tallinn, 145–160.
29. Dewri, R., Ray, I., Poolsappasit, N., Whitley, D. (2012). Optimal security hardening on attack tree models of networks: a cost-benefit analysis. International Journal of Information Security, 11 (3), 167–188. doi: https://doi.org/10.1007/s10207-012-0160-y
30. Khouzani, M., Malacaria, P., Hankin, C., Fielder, A., Smeraldi, F. (2016). Efficient Numerical Frameworks for Multi-objective Cyber Security Planning. Lecture Notes in Computer Science, 179–197. doi: https://doi.org/10.1007/978-3-319-45741-3_10
31. Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., Smeraldi, F. (2014). Cybersecurity Games and Investments: A Decision Support Approach. Decision and Game Theory for Security, 266–286. doi: https://doi.org/10.1007/978-3-319-12601-2_15
32. Zhuo, Y., Solak, S. (2014). Measuring and Optimizing Cybersecurity Investments: A Quantitative Portfolio Approach. Proceedings of the 2014 Industrial and Systems Engineering Research Conference.
33. Buldas, A., Laud, P., Priisalu, J., Saarepera, M., Willemson, J. (2006). Rational Choice of Security Measures Via Multi-parameter Attack Trees. Lecture Notes in Computer Science, 235–248. doi: https://doi.org/10.1007/11962977_19
34. Levchenko, E. G., Prus, R. B., Rabchun, D. I. (2013). Conditions of saddle point existence in multilevel information security systems. Bezpeka informatsiyi, 19 (1), 70–76.
35. Levchenko, Ye. H., Demchyshyn, M. V., Rabchun, A. O. (2011). The mathematical models of economic management of information security. Systemni doslidzhennia ta informatsiyni tekhnolohiyi, 4, 88–96.
36. Vlasov, D. A., Sinchukov, A. V. Teoriya igr: filosofskie i metodicheskie osobennosti. Available at: https://dspace.kpfu.ru/xmlui/bitstream/handle/net/110961/mathedu2016_123_127.pdf?sequence=-1&isAllowed=y
37. Goryashko, A. P. (2014). Game Theory: From Analysis to Synthesis (Survey of the Markets Design Results). Cloud of Science, 1 (1).
38. Kotenko, I. V., Ulanov, A. V. (2006). Komandy agentov v kiberprostranstve: modelirovanie protsessov zashchity informatsii v global'nom Internete. Trudy ISA RAN, 27, 108–129.
39. Akhmetov, B., Kydyralina, L., Lakhno, V., Mohylnyi, G., Akhmetova, J., Tashimova, A. (2018). Model for a computer decision support system on mutual investment in the cybersecurity of educational institutions. International Journal of Mechanical Engineering and Technology, 9 (10), 1114–1122.
40. Yevseiev, S., Aleksiyev, V., Balakireva, S., Peleshok, Y., Milov, O., Petrov, O. et. al. (2019). Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy. Eastern-European Journal of Enterprise Technologies, 3 (9 (99)), 49–63. doi: https://doi.org/10.15587/1729-4061.2019.169527

41. 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
42. Behara, R., Huang, C. D., Hu, Q. (2007). A System Dynamics Model of Information Security Investments. ECIS 2007 Proceedings, 177. Available at: http://aisel.aisnet.org/ecis2007/177
43. Marco, C., Nizovtsev, D. (2006). Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies. Proceedings of the Fifth Workshop on the Economics of Information Security. Cambridge.

Проводиться дослідження нелінійних гідродинамічних характеристик рушійно-стернового комплексу (РСК), які вливають на точність плоского траєкторного руху автономного ненаселеного підводного апарата (АНПА). При криволінійному русі підводного апарата його РСК працює у косому потоці води, що набігає. Це призводить до зниження сили упору РСК і негативно впливає на керований траєкторний рух підводного апарату. Дослідження було проведено для конкретного типу АНПА для режиму плоского криволінійного руху.

У якості методу дослідження було обрано метод математичного моделювання. З цією метою відому математичну модель руху АНПА доповнено системою керування, що імітує траєкторний рух АНПА. Розроблена модель складається з чотирьох основних блоків: удосконаленої моделі АНПА; блоку завдання швидкості руху апарату; блоку керування кутом повороту насадки; блоку, який містить заздалегідь підготовлені траєкторії руху АНПА.

Представлено результати дослідження гідродинамічних параметрів АНПА для декількох типових траєкторій його руху. До досліджуваних параметрів належать наступні: необхідний кут повороту насадки; дійсна траєкторія руху апарату; швидкість руху апарату; момент на валу гребного електродвигуна; упор гребного гвинта.

В результаті проведених досліджень побудовано діаграму залежності упору гребного гвинта від кута повороту насадки АНПА в діапазоні швидкості від 0,2 м/с до 1 м/с та при повороті насадки в діапазоні до 35°. Сформовано трьохвимірну матрицю, яка описує залежність упору гребного гвинта від кута потоку води, що набігає, та швидкості руху апарату. Отримана залежність може бути використана при синтезі регуляторів систем автоматичного керування плоским маневровим рухом АНПА підвищеної точності

Ключові слова: автономний ненаселений підводний апарат, рушійно-стерновий комплекс, математичне моделювання, поворотна насадка

UDC: 681.52: 629.5
DOI: 10.15587/1729-4061.2019.176673

MATHEMATICAL MODELING OF AUTONOMOUS UNDERWATER VEHICLE PROPULSION AND STEERING COMPLEX OPERATION IN OBLIQUE (BEVELED) WATER FLOW

V. Blintsov
Doctor of Technical Sciences, Professor,
Vice-Rector of the Scientific Work*
E-mail: volodymyr.blintsov@nuos.edu.ua
H. Hrudinina
Lecturer
Department of Electrical Engineering of
Ship and Robotic Systems*
E-mail: hanna.hrudinina@nuos.edu.ua
*Admiral Makarov National University of Shipbuilding
Heroiv Ukrainy ave., 9, Mykolaiv, Ukraine, 54025

Received date 18.06.2019
Accepted date 29.07.2019
Published date 28.08.2019

1. Introduction

Today, in the world leading maritime countries, autonomous underwater vehicles (AUVs), which differ significantly by architectural and design type, mass-dimensional parameters and depths of application, are being created. However, all varieties of AUVs combine a common property – the ability of controlled trajectory (plane or spatial) motion.

The forces acting on the underwater vehicle during such motion determine its dynamics and essentially influence the vehicle manoeuvrability. Only by having the complete information about all the forces affecting the AUV, as well as about their control means, the conditions under which it is possible to construct vehicle effective automatic control systems, can be determined.

That is why, in recent years, more and more attention is being paid to the research and improvement of the PSC auto-