Multifactorial Model of the Confrontation of Financial Resources of the Parties in Targeted Attacks

Valerii Lakhno [1], Volodimir Malyukov [1], Inna Malyukova [2], Bakhytzhan Akhmetov [3], Zhuldyz Alimseitova [4,*], and Moldir Ydyryshbayeva [5,*]

[1] Department of Computer systems, Networks and Cybersecurity, Faculty of Information Technology, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
[2] Rating Agency "Expert-rating", Kyiv, Ukraine
[3] Department of Informatics and Informatization of Education, Institute of Mathematics, Physics and Computer Science, Kazakh National Pedagogical University named after Abai, Almaty, Kazakhstan
[4] Department of Cybersecurity, Satbayev University, Almaty, Kazakhstan
[5] Department of Information Systems, Faculty of Information Technology, Al-Farabi Kazakh National University, Almaty, Kazakhstan
Email: valss21@ukr.net (V.L.); volod.malyukov@gmail.com (V.M.); imalyukova82@gmail.com (I.M.); bakhytzhan.akhmetov.54@mail.ru (B.A.); zhuldyz_al@mail.ru (Z.A.); moldir.ydyryshbaeva@gmail.com (M.Y.)
*Corresponding author

***Abstract*—A multifactorial model of countering targeted attacks (Advanced Persistent Threats (APT) attacks) is considered in the context of available financial resources within the framework of a bilinear multistep quality game with several terminal surfaces. The distinguishing feature of the proposed model is its incorporation of multivariance in financial strategies for safeguarding against APT attacks and counterattacks, which is manifested in the dynamics of interaction between opposing sides. This facilitates the consideration of the overarching problem of cyber defense within the framework of the game scheme, encompassing the tasks of countering APT attacks with the financial resources available to the defense side. The proposed solution to the problem entailed the implementation of a bilinear multistep game of the quality of multidimensional objects. The resolution of quality issues, considering their multidimensionality and the bilinearity of the dynamics of player interaction, is a rather challenging problem. However, the formulated problem was solved in the paper by employing the optimality principle of R. Bellman. The solution was identified within the framework of a positional multistep game scheme with complete information. A comprehensive investigation was conducted to ascertain the optimal strategies for allocating the financial resources of the first player to build a system of protection against targeted attacks. The model delineated in the paper was implemented in the form of a software module of an intelligent information system. The results of a computational experiment that was conducted to test the model's operability are presented herein.**

***Keywords*—multistep quality game, preference set, optimal strategy, targeted cyberattack, financial resources**

I. Introduction

As Information Technologies (IT) become increasingly complex and more deeply integrated into the business processes of various companies and organizations (which we will designate as Objects of Informatization (OI) in this study), the methods employed by cyberattackers in orchestrating cyberattacks are also evolving. The vector of attacks will be diversified, with an increasing destructive impact on the components of the OI technological infrastructure. It has been demonstrated that traditional attacks, including DDoS, phishing, and brute-force attacks, represent merely a fraction of the intricate framework comprising targeted cyberattacks (APT, or Advanced Persistent Threats) [1, 2]. The repercussions of such targeted attacks (i.e., APT attacks) on the OI can be disastrous. For consistency and to avoid confusion, all targeted persistent attacks of this type are referred to in the text as APT attacks.

It is important to acknowledge that the Information Security Tools (IST) employed by the defense side to neutralize conventional threats to Information Security (IS) frequently lack effectiveness against APT attacks. This phenomenon can be attributed to the strategic focus of cyber-attackers (hereinafter referred to as the "attacking side") on specific objectives. Furthermore, attackers possess the capability to adjust their methods of conducting an APT attack in accordance with the protective measures and means implemented. However, this results in an increase in the cost of protecting the OI when conducting this kind of APT attack by the attacking party. Accordingly, as demonstrated in Dan's [3] study, the

Manuscript received February 23, 2026; revised March 18, 2026; accepted May 29, 2026; published August 19, 2026.

financial expense associated with orchestrating a cyberattack remains substantially lower compared to the financial investment required for safeguarding the target.

Hua and Bapna [4] addressed certain aspects of the issue by evaluating the economic implications of hacker attacks. Additionally, Olech's [5] study provides data relevant to the estimation of the cost of work by cyber-disruptors. According to Dan [3], Hua and Bapna [4] found that the investments of cyberattackers are immediately rewarded after the initial successful cyberattack. Conversely, as the degree of security of the OI increases, the number of successfully implemented attacks experiences a steady decrease. Concurrently, the financial expenditure associated with the utilization of hacking tools remains consistent [3].

In order to optimize their costs for organizing attacks, especially if we are talking about targeted attacks (which include many stages and performers), the attacking side must look not only for ways to increase the effectiveness of attacks.

The offensive side is also endeavoring to minimize the cost of procuring malicious software, preferring instead to exploit the prevailing vulnerabilities of the OI.

If the attacking side possesses at least approximate data concerning the cost of conducting an APT attack, they will be capable of predicting the potential financial return of such an attack. However, such forecasts or calculations of the payback of the attack are rendered meaningless if the defense side is opposed by the special services or the cyber army of the enemy during the APT attack. In the case of the latter, the notion of the cost of conducting an attack is rendered meaningless. Ultimately, their primary objective is the achievement of their goals. As previously demonstrated, such objectives may encompass the withdrawal from a workable state or the complete destruction of the information infrastructure of the APT-attack object.

In the event that an Advanced Persistent Threat (APT) attack is executed by cybercriminals who have been contracted by criminal organizations or business competitors, the customer's investment in such an attack is likely to yield a positive return. Conversely, failure to do so by the party initiating the transaction (i.e., the customer and the performers) will result in financial losses for said party.

The resolution of the problem of choosing rational financial strategies to prevent APT attacks on the OI is a complex scientific and practical task.

It is the position of the defense side that effective tools are required for the forecasting and evaluation of options for strategies for investing Financial Resources (FR) in IS OI projects. Such tools may include Intelligent Information Systems (IIS) capable of automating the search for analytical solutions to this problem.

The most effective approach to resolving the problem of the confrontation of the resources of the parties opposing each other during the APT attack on the OI is the use of the game theory apparatus. The allocation of financial resources among the parties is determined by the interaction between the defending and attacking sides. The present discussion pertains to the relationship between decisions made by information security management regarding the financing of information security systems and the financing of tools utilized by attackers. In the context of this interaction, each of the parties involved can be regarded as a participant in the game. The OI Information Security Manager (the first player) seeks to identify the optimal strategy for allocating Financial Resources (FR) to protect OI information assets. The second player, designated as the "attacking OI," endeavors to distribute his FR in a manner that optimizes its allocation to the designated stages of the APT attack.

It is well-documented that the utilization of bilinear multistep games is an effective solution method for such problems [6]. The bilinearity of such games is attributable to the distribution of FR players to complete their assigned tasks. Conventionally, the optimality principle of R. Bellman is employed to address such games [7]. Concurrently, identifying an explicit solution, particularly in the context of multidimensional variables—a subject that this paper explores—constitutes a highly non-trivial undertaking. Consequently, the problem of the optimal distribution of the FR protection of the OI and the attackers, as contemplated in the paper, is pertinent. The solution to the problem is of great practical interest when analyzing the capabilities of the parties involved in achieving their objectives during an APT attack. The explicit form of the solution is particularly relevant in this context.

II. Literature Review

For the entity initiating the offensive, if the primary objective is to generate profit as a consequence of the attack, it is imperative to address the following inquiries: what is the estimated cost of an APT attack, and what are the necessary financial resources and participants for its preparation and execution? In the event that the APT attack is prolonged, the financial implications of its implementation will be substantial. It is imperative to acknowledge the inherent challenges in operating with precise numerical values. This is due to the fact that, even at the exploratory stage, a considerable discrepancy is observed in the cost of various tools necessary for implementation. Furthermore, it is impossible to ascertain the amount of compensation that the specialists hired by the attacking side will receive for their services, such as the creation of unique software for hacking the target OI system. It should be noted that approximate estimates are available. For instance, the cost of hacking a server using a program that retrieves passwords is approximately $175.00 per week. A malware development service can cost a minimum of $300.00 per project, and a malware development and reverse engineering service can cost a minimum of $600.00 per project [3]. However, it is important to note that cybercriminals may allocate significantly different budgets for conducting an APT attack. Furthermore, the budget allocated for each subsequent stage of such an attack is correlated with the success of the previous stage. The financial incentives

offered by APT attacks are contingent upon the magnitude and efficacy of the tasks they successfully execute.

It is posited that the cost of an attack is contingent upon a number of factors, including the rate of a particular specialist involved in the attack, the nature of a specific task, and the complexity of the code (in the context of developing unique hacking software). It has been demonstrated by the investigation of numerous APT attacks that the majority of the software utilized for a given hack is typically developed by the attack participants themselves. The deployment of such malware is a one-time occurrence, utilized exclusively during a targeted attack. Conversely, this has the potential to increase the cost of development. Conversely, such malware can evade detection by existing information security systems.

As demonstrated in Dan's [3] research, the range of prices for services and software utilized in numerous APT attacks is substantial. The landscape of the hacker services market is undergoing a period of dynamic transformation. Furthermore, in the event that the attackers have identified a novel vulnerability and have developed an exploit for it, the price of such an exploit can fluctuate significantly, ranging from hundreds to thousands of dollars, until the vendor issues a resolution for the vulnerability. Following the identification of a vulnerability by the vendor and the implementation of a patch to address it, there is a significant reduction in the financial cost associated with the exploitation of the vulnerability. However, even the exploitation of previously discovered vulnerabilities can yield advantages for the attacker.

It is evident that a considerable number of companies continue to exhibit a lack of seriousness regarding information security concerns. Furthermore, there appears to be a lack of urgency in allocating financial resources to address these vulnerabilities. Consequently, this results in the creation of vulnerabilities that can be exploited by attackers to gain access to the target system. This phenomenon results in the prolonged vulnerability of the OI to attacks by exploiters with assets valued at less than $100.

According to the data set compiled by Dan [3], the average total cost of an APT attack is estimated to range from 10,000 to 15,000 dollars. While APT attacks on large international holdings are documented, the financial cost of these attacks has been reported to exceed 300,000 to 500,000 dollars.

Many researchers addressing the issue of optimizing investments in information security reasonably assume that the decision should be based on weighing the costs of building an information security system for the OI and the benefits received [8–10]. The authors of these papers regarded the theory of decision-making as a vital element in supporting the objective of rational investment in information security.

In a recent study [11], a novel model was proposed. This model enables the analysis of the costs and benefits associated with various strategies for investing in the cybersecurity of smart home residents. The authors employed evolutionary game theory to model a game comprising three populations. These categories include smart home users, interested parties, and intruders. In their study of the non-cooperative game, the authors meticulously analyze the costs and advantages associated with both the defense and the attacker's strategies.

Cavusoglu, Cavusoglu *et al.* [12] demonstrated that game theory approaches are more suitable for the problem of investing in information security than traditional approaches of decision theory. This is particularly salient when considering the propensity of cybercriminals to exhibit creativity in their methods and to frequently modify their tactics. Attackers have the capacity to utilize diverse entry points into the OI computer systems [13, 14].

This finding lends further credence to the notion that the employment of a game-theoretic approach is a rational and effective strategy for addressing the research problem under consideration in this study.

In Ref. [15], a game model was presented that determines the optimal size of investments in cyber security for sellers seeking to maximize expected profit. This model impacted a relatively limited segment of cyberattacks experienced by sellers of diverse products. The authors' primary focus is on the benefits that buyers derive from the heightened level of information security in the market.

Nagurney *et al.* [16, 17] proposed models based on the application of the mathematical apparatus of game theory and taking into account the impact of investments in the cyber security of the supply network. It is important to note that these works do not consider the possibility that the entity initiating a cyber attack may also increase the financial costs associated with the attack. For instance, attackers have the capability to procure ready-made software or to commission unique software capable of causing harm to the target system. This circumstance is important for assessing the costs and benefits of investing in IS. Tosh *et al.* [18] proposed a sequential game model that includes three players. In this case, the entity in question is the organization itself, the attacker, and the insurer. The authors utilize the model to analyze the optimal investment strategy of self-defense for organizations, the optimal attack speed for the enemy, and the optimal level of coverage of insurers using numerical results. However, the proposed game operates under the assumption that all players are privy to the moves of the other players.

Such a scenario is not entirely realistic. So, when conducting APT attacks, most of the attacked at the initial stages of the attack, do not even know about its beginning.

In Ref. [19], a game-theoretic approach is proposed to optimize cybersecurity investment strategies in smart grids. The model is predicated on the assumption that the costs of attacking intruders and defending against the attack of defenders are known. Furthermore, the assailants endeavor to minimize their expenditures by maximizing the expenditures of the defenders, and, conversely, for the defense. However, the authors' model does not take into account the potential financial benefits that could be accrued by the defense sector when selecting the most optimal strategy for investing in cyber security. This is a

critical component in evaluating the significance of the selected investment strategy.

Sun *et al.* [20] utilize evolutionary game theory to examine investments in information security within the mobile e-commerce industry. The model incorporates a penalty parameter. The regulation of this parameter is expected to stimulate investment in IS.

A comparable approach was proposed in Ref. [21]. However, the analysis was limited to a static model of the game, neglecting to consider the evolution of players' strategies over time. As previously indicated, the strategies employed by intruders are subject to constant evolution.

Grossklags *et al.* [22] proposed a two-stage model aimed at assisting the defense sector in making a decision regarding the optimal allocation of the OI budget for cyber security. The authors demonstrate the potential for a scenario characterized by "strategic uncertainty" among the parties involved. In this case, the defense party seeks to protect its information assets only slightly above the lowest acceptable level.

Musman and Turner [23] presented an analysis of hybrid game-theoretic and optimization approaches to the allocation of the OI budget for the provision of information security. The authors of the study compared three different approaches to allocating the budget for the IS OI. The emphasis was placed on the use of decision support systems.

Korzhyk *et al.* [24] describe a game-theoretic model in which the functions of the costs of providing information security are considered. The value of this function is subject to variation depending on the level of security of the OI.

In the study by Srinidhi *et al.* [25], an optimization model was developed that enabled the authors to determine the allocation of resources to information security based on the value of information assets.

Cavusoglu *et al.* [12] compared approaches to the issue of investing in information security based on the theory of decision-making and on the basis of game theory. However, the authors did not investigate the optimal set of OI protection tools.

Rass *et al.* [26] focused on the calculation of equilibrium in strategies for the attacker-defender game. However, the authors did not address the question of how the choice of a particular defense and attack strategy, in particular, for complex, long-term and multi-stage APT attacks, will affect the costs of the parties participating in the conditional game. This work did not consider the selection of a rational strategy from the perspective of investing in attack and defense.

In Ref. [27], a deliberate review and analysis of the extant literature on the methods of game theory was conducted, including in relation to the issues of investing in IS OI. The authors have classified these methods according to the security policies that have been adopted for the OI.

It is this author's opinion, based on the available evidence, that game theory is most consistent with the task of modeling conflict and cooperation between persons (players) involved in the APT attack or its individual stages. Game theory has the potential to enhance the security of information for a wide range of OIs. From our perspective, game theory offers the most consistent framework. This predetermined our interest in this area of research. However, it should be noted that, despite the extensive body of research devoted to the economics of information security, this methodology generally lacks comprehensiveness in modeling protracted, multi-stage APT attacks. Most of the studies analyzed above and their authors either limited themselves to single-stage games, ignoring the depletion of the parties' budgets during the confrontation, or relied on models with complete certainty. These authors ignored the variability in the market value of exploits and protective measures at different stages of an incident. The main research gap is the current lack of analytical tools that allow the defender to recalculate the optimal allocation of financial resources directly during the escalation of an APT attack. This study aims to address this methodological limitation by introducing the concept of multivariate financial strategies. In this paper, we endeavor to present our vision for resolving this issue by employing the theoretical framework of game theory. To address this challenge, the toolkit of bilinear multistep quality games with multiple terminal surfaces is employed [28]. This phenomenon can be attributed, first and foremost, to the effective utilization of the FR distribution procedure in both the OI defense and the attacking sides during the APT attack.

The objective of the present study is to develop mathematical models that constitute the computational core of an Intelligent Information System (IIS) used to analyze the parties' capabilities to implement targeted cyber attacks.

During the course of the study, the following tasks were addressed:

(1) The development of a model for finding optimal financial strategies of players during an APT attack is based on game theory (multistep quality game). The resolution of such a problem contributes to the analysis of the situation by countering the side that attacks the OI with the help of a targeted APT attack.
(2) The execution of computational experiments is facilitated by the Python programming language.

III. Materials and Methods

The issue of ensuring information security has emerged as a paramount concern within the domain of information technology. The multitude of methods employed in attacks on the OI, particularly during the execution of meticulously orchestrated APT attacks across multiple stages, necessitated the development of commensurate protective measures (see Fig. 1). The hypothesis that the effective and reliable protection of the OI, including from APT attacks, is impossible without financial support of the parties to the conflict interaction is not contingent upon special evidence. The necessity of FR for the attacking side, or, from a game-theoretical perspective, the attacking player, is a critical consideration. FR is allocated for the development of tools utilized in various phases of an APT attack. Personnel engaged in reconnaissance activities, the

installation of malicious software within the target environment, and other related operations are compensated. The OI protection player requires FR to procure and implement protection tools and to remunerate personnel of information security units.

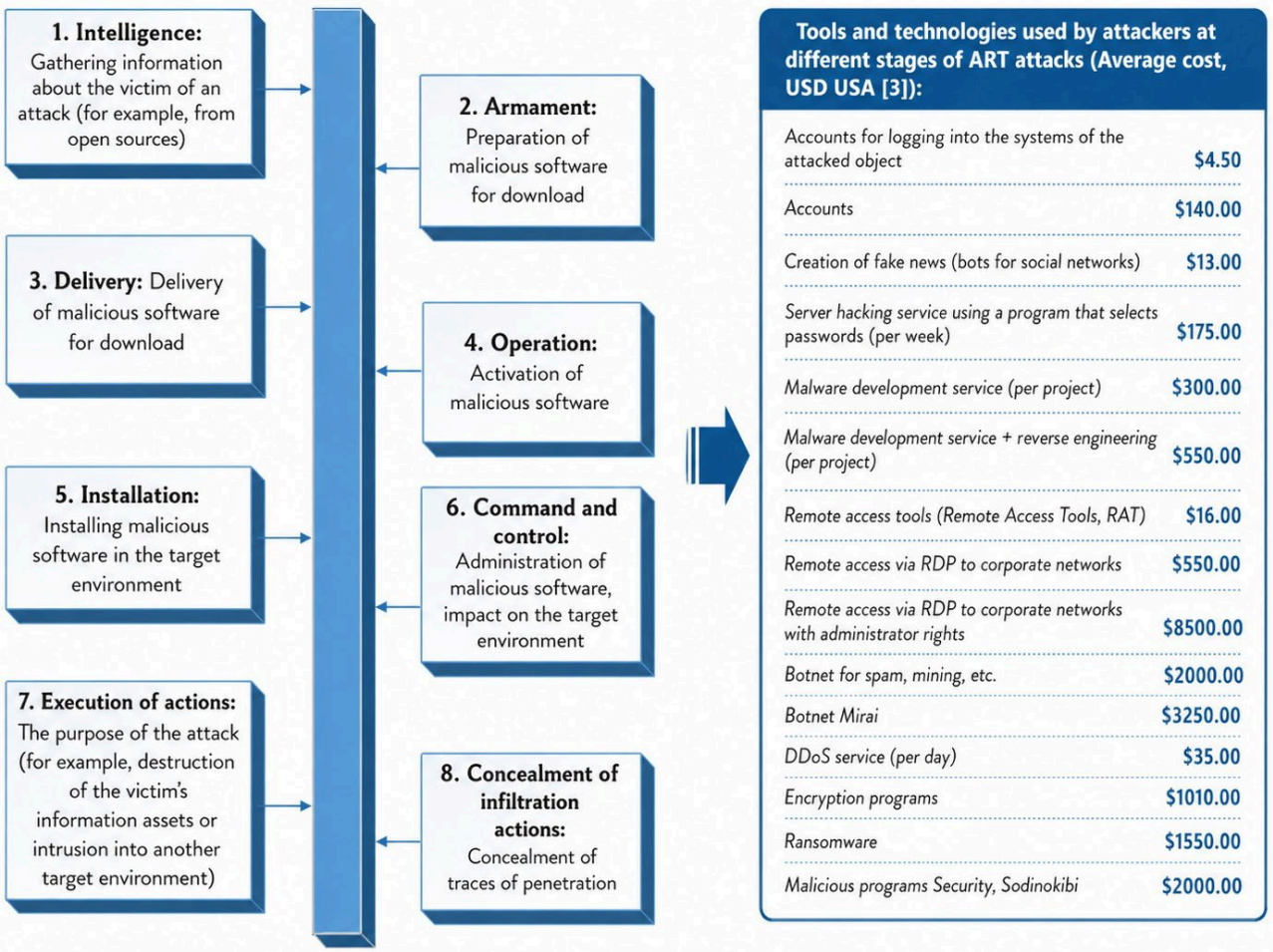

Fig. 1. The scheme of the APT attack with an approximate list of the attacking party's tools.

As previously indicated, the OI defense player will be regarded as the first player. Consequently, the player initiating the attack on OI is designated as the second player. Given that both sides incur financial costs during the course of long, multi-stage APT attacks, it is possible to discuss the financial interaction of the players representing the sides of defense and attack. From the perspective of the "consumability" of the APT attack and protection against it, such interaction is due to the interdependence of the FR players.

Such interaction is a discrete-time procedure. The interaction manifests as follows. The initial player has developed technological strategies to counter the APT attacks of the second player. This encompasses the identification of anomalies in OI computer systems, the utilization of sandboxes to emulate OI workstations, and the surveillance of network activity. In order to inflict harm upon the first player, the second player has been endowed with technological strategies. These strategies encompass the following: the collection of information about the victim from public sources, the creation of unique malware for the implementation of an APT attack, the employment of social engineering methods, and the adaptation of malware to the target environment. It is important to note that the coincidence of the number of alternatives does not affect the essence of the problem. It is important to note that these two concepts may not align, which simplifies to the scenario of equal numbers of alternatives. The employment of technological strategies by the second player results in financial losses for the first player. The financial costs associated with the construction of an information security system can serve as a deterrent, effectively impeding the success of an APT attack.

In general, the cyber attack market is characterized by a high degree of organization. The existence of a similarity in the pipeline among different stages of APT attacks is a plausible proposition. In the context of a performance, the allocation of responsibility for each stage is determined by the respective performers. Furthermore, there are instances in which less qualified hackers transmit the results of their work to more qualified hackers. Conversely, the former prioritize the financial compensation for their services [29].

So, we believe that any strategy of the second player leads to financial losses. Let the second player apply his i −strategy in the established financial system. The use of

this strategy brings the first player financial damage in the amount of ω_i^1. Next, let the first player (defender of the OI) apply his $j-$strategy in the established financial system. The application of this strategy brings financial benefits in the amount of ω_j^2. Denote by d_{ij}^1 the relation ω_i^1/ω_j^2, and by d_{ij}^2 the relation ω_j^2/ω_i^1. If $\omega_i^1 = 0$ for some i or $\omega_j^2 = 0$ for some j, then we exclude such strategies from consideration. Denote by D_1 a matrix consisting of elements of D_{ij}^1. The number of rows corresponds to the number of alternatives of the second player, and the number of each row corresponds to the corresponding alternative of the second player. By D_2 we denote a matrix in which the rows correspond to the alternatives of the first player, and the columns correspond to the alternatives of the second player, i.e. the elements of d_{ij}^2 mean that they are in the j row and i column.

It should be noted that matrices D_1 and D_2 are analogs of the so-called profitability matrices, each element of which characterizes, for example, for matrix D_1, what amount of losses from the use of the attacking player's technological strategy is compensated by a unit of income from the use of the defender player's technological strategy and vice versa. It is this circumstance that makes it possible to form the dynamics of interaction between the opposing sides.

The first player, having at time $t = 0$ $\mu(0) \in R_+^K$ Financial Resources (FR), converts them to the value of resources $H_1 \times \mu(0)$. H_1 is the transformation matrix of the FR resources of the first player of order K, with positive elements. Then he determines the value of his investment $U(0) \times H_1 \times \mu(0)$ by selecting the elements $u_i(0): 0 \le u_i(0) \le 1$, being the diagonal elements of the diagonal matrix $U(0)$ of order K, which determine the values of the strategy of the first player. Such an investment by the first player means that it allows compensating for $D_1 \times U(0) \times H_1 \times \mu(0)$ losses from the actions of the second player.

The second player acts similarly. The second player, having at time $t = 0$ $\eta(0) \in R_+^K$ financial resources, converts them to the value of resources $H_2 \times \eta(0)$. Here H_2 is the transformation matrix of the FR of the second player of order K, with positive elements. Then he determines the value of his investment $V(0) \times H_2 \times \eta(0)$ by selecting elements $v_i(0): 0 \le v_i(0) \le 1$, that are diagonal elements of the diagonal matrix $V(0)$ of order K, which determine the values of the strategy of the second player. Such an investment by the second player means that it allows leveling $D_2 \times V(0) \times H_2 \times \eta(0)$ of income from the actions of the first player.

Then the FR of the players at time $t = 1$ will be written as follows:

$$\begin{aligned}\mu(1) &= H_1 \times \mu(0) - U(0) \times H_1 \times \mu(0) - D_2 \times V(0) \times H_2 \times \eta(0)\\ \eta(1) &= H_2 \times \eta(0) - V(0) \times H_2 \times \eta(0) - D_1 \times U(0) \times H_1 \times \mu(0)\end{aligned} \quad (1)$$

At time $t = 1$, the following options are possible:

$$\big(\mu(1), \eta(1)\big) \in S_0, \quad (2)$$

$$\big(\mu(1), \eta(1)\big) \in F_0, \quad (3)$$

$$\big(\mu(1), \eta(1)\big) \in D_0, \quad (4)$$

$$\big(\mu(1), \eta(1)\big) \in H_0, \quad (5)$$

where S_0, F_0, D_0 and H_0 such:

$$S_0 = \bigcup_{i=1}^{K} \{(\mu, \eta): (\mu, \eta) \in R^{2K}, \mu \ge 0, \eta_i \prec 0\},$$

$$F_0 = \bigcup_{i=1}^{K} \{(\mu, \eta): (\mu, \eta) \in R^{2K}, \mu_i \prec 0, \eta \ge 0\},$$

$$D_0 = \{\bigcup_{i=1}^{K} \{(\mu, \eta): (\mu, \eta) \in R^{2K}, \mu_i \prec 0\}\} \cap \{\bigcup_{i=1}^{K} \{(\mu, \eta): (\mu, \eta) \in R^{2K}, \eta_i \prec 0\}\},$$

$$H_0 = \bigcup_{i=1}^{K} \{(\mu, \eta): (\mu, \eta) \in R^{2K}, \mu \ge 0, \eta \ge 0\}.$$

In the presented Eqs. (1)–(5), the parameters have the following economic interpretation. State variables describe the remaining budget of each party at the current point in time. The diagonal elements of the control matrices formalize the shares of investments allocated to specific technological strategies. The transformation matrices act as weighting coefficients that reflect the market value of neutralizing one unit of damage. Thus, condition Eq. (2) captures a situation of complete financial exhaustion of the attacker while the defender remains operational, which is interpreted as a successful repulsion of the threat.

That is, with $H_0 = \cup_{i=1}^{K} \{(\mu, \eta): (\mu, \eta) \in R^{2K}, \mu \ge 0, \eta \ge 0\}$.

Case Eq. (2) is desirable for the first player. Case Eq. (3) is desirable for the second player. In case Eq. (4), the players also stop interacting, since they cannot continue it. In case Eq. (5), they continue the interaction for the moments of time $t \succ 1$.

Matrices Φ_k and Ψ_k are intended to record the first player's preference sets and his "guarantee against defeat" set by the second player.

The solution to the game under consideration was based on R. Bellman's principle of dynamic programming. It consists of the following stages.

(1) Stage 1.

We assume a one-step game. We assume that the players make one step given the initial states $x(0)$ and $y(0)$. Since the end of the game in one step is already specified, using the notation $x(1)$ and $y(1)$. This entry defines the interaction dynamics. Next, we determine the

optimal actions of the players, which are selected taking into account the coefficients for the states $x(0)$ and $y(0)$.

A multifactorial procedure for countering targeted APT attacks will be considered within the framework of a positional multistep quality game with complete information.

Due to the symmetry, we will limit ourselves to considering the problem from the position of the first defending player. The second task is solved similarly.

The definition of pure strategy and the preference set of the first player was previously given in Ref. [18].

When a problem is regarded from the vantage point of the first player, as per the principles of game theory, this approach is understood as a resolution of the problem from the perspective of the first player (the ally). The second player is designated as the opposing player. The distinguishing factor among these players is their level of information status. The ally is privy to the state of the game at any given moment, while the adversary has access to all the information.

Accordingly, the problem should now be considered from the perspective of the first ally player. Given the complete symmetry of the problem from the perspective of the second ally, it will not be considered here.

In a one-step game, the first player chooses his control in such a way that there are as many states $x(0)$ and $y(0)$ as possible that have the property that the first player will achieve his goal, no matter what the second player (opposing player) does. He can do this by choosing his control, which depends on the coefficient at state $x(0)$. Since the second player is interested in having as few such states as possible, he chooses his control based on these considerations.

(2) Stage 2.

We assume that the game has two steps. In this case, we assume that states $x(1)$ and $y(1)$ are such that the first player achieves the goal in one step. This means that this set is described as the set of states found in the first stage. Then, states $x(0)$ and $y(0)$ will be such that the game, after two steps, will develop such that the first player will move to the set found in the first stage. In this case, the first player will choose his control at the first step in such a way that there will be as many such states $x(0)$ and $y(0)$ as possible, no matter how the second player acts, then the preference set of the first player will be found in two steps.

It should be noted that the choice of controls for both the first and second players depends on the coefficients, or rather on the signs of the coefficients in states $x(0)$ and $y(0)$. This means that the controls take either the maximum value or the minimum value.

Stage k. The exact same procedure will occur at step k. This is nothing more than an implementation of the principle of dynamic programming, as applied to the problem considered in this article.

Let's return to the question of where the matrices Φ_k and Ψ_k came from. These matrices define the preference sets of the first ally player at the k-th step. Since the choice of players' controls depends on the signs of the elements of the matrix rows that are in the state dynamics record to the left of the players' controls, which are diagonal matrices, it is necessary to determine when it will be possible to switch the corresponding element of the diagonal control matrix from one value to another, for example, from the maximum value to the minimum value or vice versa. To achieve this, coefficients were introduced as fractions. Taking these fractions into account, a theorem was formulated that allowed conclusions to be drawn about the possible outcome of this interaction between the players.

IV. Result and Discussion

A multifactorial procedure for countering targeted APT attacks will be considered within the framework of a positional multistep quality game with complete information.

Due to the symmetry, we will limit ourselves to considering the problem from the position of the first defending player. The second task is solved similarly.

The definition of pure strategy and the preference set of the first player was previously given in Ref. [18].

The preference set of the first player is the set of initial states of the players $(\mu(0), \eta(0)) \in R_+^{2K}$ having property (A).

Property (A): A set of states $(\mu(0), \eta(0)) \in R_+^{2K}$, for which there is a strategy $U_*(.,.,)$ of the first player, the use of which ensures that condition Eq. (2) is fulfilled at one of the moments of time k.

At the same time, this strategy guarantees that conditions Eqs. (3) and (4) are not fulfilled at previous points in time.

The set of such states will be called the preference set of the first player Δ_1. Accordingly, the strategies $U_*(.,.,.)$ of the first player having the specified properties are his optimal strategies.

The solution to problem 1 consists in finding the sets of "preference" of the first defending player and his optimal strategies. Similarly, the task is set from the point of view of the second player-an ally.

A. Solution of Problem 1

The solution of the problem depends on the ratio of the parameters that determine the procedure of confrontation between the defending player and the second opponent player.

Let's introduce such notation.

Denote by $\widehat{\Delta_1}$ the set:

$$\widehat{\Delta_1} = \Delta_* - \bigcup_{i-1}^{K} \Delta_i,$$

$$\Delta_* = \begin{Bmatrix} (\mu(0), \eta(0)) : (\mu(0), \eta(0)) \in R_+^{2K}, \\ H_1 \times \mu(0) - D_2 \times H_2 \times \eta(0) \in R_+^K \end{Bmatrix},$$

$$\Delta_i = \begin{Bmatrix} (\mu(0), \eta(0)) \in R_+^{2K}, \\ (H_1 \times \mu(0))_i = (D_2 \times H_2 \times y(0)))_i, \\ i = 1, \dots, K; \end{Bmatrix}.$$

Further, the following designations are additionally introduced:

E −the unit matrix of order K.

$$\Phi_1 = D_1,$$

$$\Phi_k = \{(\Psi_{k-1} \times H_2 \times D_1 - \Phi_{k-1} \times H_1)^+ + \Phi_{k-1} \times H_1\},$$

$$\Psi_1 = E + D_1 \times D_2,$$

$$\Psi_k = (\Phi_{k-1} \times H_1 \times D_2 - \Psi_{k-1} \times H_2)^+ + \Psi_{k-1} \times H_2 +$$

$$(\Psi_{k-1} \times H_2 \times D_1 - \Phi_{k-1} \times H_1)^+ D_2, \qquad k = 2, \ldots$$

$$x^+ = \begin{cases} x, & x \geq 0; \\ 0, & x \prec 0; \ x \in R; \end{cases}$$

$$\sigma_j^{k,j} = \begin{cases} 1, & (\Psi_k \times H_2)_{ij} = 0, \\ \dfrac{(\Phi_k \times H_1 \times D_2)}{(\Psi_k \times H_2)_{ij}}, & (\Psi_k \times H_2)_{ij} \neq 0, \ k = 1, \ldots \end{cases}$$

The process of constructing the preference sets of the first player depends on the ratio of the parameters that determine this conflict interaction.

Consider the case $H_1 \times D_2 \geq D_2 \times H_2$.

Let us assume that the condition is met under which a basic budget ratio exists. However, inequality Eq. (6) is not satisfied.

$$(\Phi_k \times H_1 \times D_2)_{im} \geq (\Psi_k \times D_2)_{im}, 1 \leq i \leq K, \quad 1 \leq m \leq K; k = 1,2, \ldots \tag{6}$$

The physical meaning of this inequality violation is that the defender's current financial resources are insufficient to guarantee the system's transition to a terminal state—a defense win at the current game step. Mathematically, this means that the defense's budget does not dominate the attacker's costs, taking into account the resource transformation matrices. Consequently, the process of constructing preference sets cannot be completed instantly and requires moving on to the analysis of the next time step, i.e., an increase in the game planning horizon.

Then the process of constructing preference sets continues in time and the preference sets of the first player will be a countable number. Based on the principle of optimality of R. Bellman, the preference sets of the first player are "built" step by step—first, the preference set is built in one step, then in two steps, etc.

Thus, there is a preference set of the first defending player, namely, this set Δ_1 is the union of preference sets Δ_1^k for a specific number of steps, i.e.,

$$\Delta_1 = \bigcup_{k=1}^{\infty} \Delta_1^k$$

Note that we mean that we construct the preference sets of the first defending player Δ_1^k in a specific number of steps, the combination of which will give the desired preference set Δ_1 of the first defending player [30].

Within the framework of the above notation, the entry of optimality sets Δ_1^k looks like this:

$$\Delta_1^k = \bigcup_{i=1}^{k} \{(\mu(0), \eta(0)) : (\mu(0), \eta(0)) \in R_+^{2K},$$

$$H_1 \times \mu(0) - D_2 \times H_2 \times \eta(0) \in R_+^K,$$

$$(\Phi_k \times H_1 \times \mu(0))_i \succ (\Psi_k \times H_2 \times \eta(0)_i\}.$$

The optimal strategy $U_*(.,.,.)$, which is determined by the elements $u^*(.) = (u^{*,1}(.), \ldots, u^{*,K}(.))$ of the first defending player, which are diagonal elements of the matrix $U_*(.,.,.)$, in the region of preference Δ_1^k is written as follows:

$$u^{*,j}(\mu, \eta) = \begin{cases} 1 - \left[\dfrac{(D_2 \times H_2 \times \eta)_j}{(H_1 \times \mu)_j}\right], \\ if \ (D_1 \times \mu)_j \succ (D_2 \times H_2 \times \eta)_j; \\ a \in [0,1] \ if \ (H_1 \times \mu)_j = 0, \\ (H_1 \times \mu)_j \geq (D_2 \times H_2 \times \eta)_j; \\ 0, otherwise; \\ (\mu, \eta) \in R_+^{2K}; j = 1, \ldots, K. \end{cases}$$

The preference sets and optimal strategies of the first defending player in the case of: $\neg(H_1 \times D_2 \geq D_2 \times H_2)$ are found in a similar way.

We present without proof the theorem [28], which provides conditions that determine the possibility of completing the procedure of interaction of players in a finite number of steps.

B. The Theorem

In area $\widehat{\Delta_1}$, the first player can reach the goal:

(1) for a finite number of steps i.e. $\widehat{\Delta_1} \subseteq \bigcup_{k=1}^{N_*} \Delta_1^k, 0 < N_* < +\infty$
if $\lim_{T \to \infty} \left(\min_{1 \leq k \leq K} \left(\sigma_k^{T,i} \right) \right) > 1$, with some i: $1 \leq i \leq K$;

(2) at least by a countable number of steps (or $\widehat{\Delta_1} \subseteq \bigcup_{k=1}^{\infty} \Delta_1^k$),
if $\lim_{T \to \infty} \left(\min_{1 \leq k \leq K} \left(\sigma_k^{T,i} \right) \right) = 1$, with some i: $1 \leq i \leq K$;
It is possible that in area $\widehat{\Delta_1}$, the first player may not reach the goal in any number of steps:

(3) where $\sup_T (\max_{1 \leq i \leq K} (\min_{1 \leq k \leq +K} (\sigma^{T,j}))) < 1$.

The proof of the theorem [30] is based on the method of backward induction (dynamic programming) and the construction of a sequence of preference sets $\Delta_1(k)$ for each step $k = N, N-1, \ldots, 0$.

(1) Induction basis. At $k = N$ (terminal step), the set $\Delta_1(N)$ is defined directly by the terminal condition Eq. (2). It represents a cone in the resource space where the budget of the first player (defender) is sufficient to fulfill the defense goals, and the resources of the second player are depleted.

(2) Induction Step. Assume that the set $\Delta_1(k+1)$ has already been constructed. Then the state $\mu(k)$ belongs

to the set $\Delta_1(k)$ if and only if there exists a control strategy $u(k) \in U$ such that for any action of the attacker $v(k) \in V$ the state of the system at the next step $\mu(k+1)$, calculated according to Eq. (1), is guaranteed to fall into $\Delta_1(k+1)$.

(3) Bilinear property. Due to the bilinear structure of Eq. (1), the mapping is continuous and preserves the convexity of sets. This allows reducing the problem of finding optimal strategies at each step to solving a local matrix game. Conditions Eqs. (2)–(4) of the theorem are necessary and sufficient conditions for the solvability of this game in pure or mixed strategies.

(4) Completion. By successively applying the inverse preimage operator from $k = N$ to $k = 0$, the final domain $\Delta_1(0)$ s formed. If the initial state of resources $(\mu_1(0), \mu_2(0))$ belongs to $\Delta_1(0)$, then according to Bellman's optimality principle, there exists a guaranteeing defender strategy. A complete mathematical justification of this construction is given in Ref. [30].

Thus, the authors found a solution to the problem of countering targeted APT attacks within the framework of the considered mathematical model. The necessary conditions are given for the completion of the process of countering targeted APT attacks in a finite time, with the available financial resources of the defense side.

C. Computational Experiment

The model described in our work was implemented in the form of an IIS software module. The computational experiment, which was conducted in order to test the performance of the model, was carried out using the Anaconda distribution (PyChar Professional programming environment).

A PC with an i7 processor and 32 GB RAM was used. The computational experiment made it possible to visualize the results of the game between the defender OI and the attacking OI. The goal is to analyze the costs of the parties during the game, simulating the costs of the parties to conduct an APT attack. The result of the game implemented during the computational experiment is shown in Table I and Fig. 2.

The basic algorithm for calculating the first player's (defender) preference region can be represented by the following pseudocode (Algorithm 1):

To conduct the computational experiment, the parameters of the profitability matrices D_1 and D_2 were formed based on real market data on the cost of APT attacks and protection tools, shown in Fig. 1. Fifteen test scenarios were selected, presented in Table I. Each scenario simulates a different initial ratio of the defender's $\mu_1(0)$ and the attacker's $\mu_2(0)$ budgets with a random distribution of the cost of exploits from \$175 to \$3000. The goal of the experiment is to test the model's sensitivity to a sharp increase in the attacker's budget. In other words, the goal is to simulate the involvement of cyber armies or state-sponsored hacker groups in the attack. Table I shows how the initial financial parameters (columns 2–4) influence the final defender preference domain $\Delta_1(0)$ (column 5), allowing to determine whether the allocated information security budget is sufficient to repel a multi-vector attack.

Algorithm 1. Calculation of the Defender's Preference Set

1: **Input**: Matrices D_1, D_2, Transformation matrices $\Phi_k, \Psi_Л$, Number of steps N
2: **Output**: Preference set $\Delta_1(0)$ and optimal strategies U^*
3: Initialize $\Delta_1(N)$ based on terminal condition Eq. (2)
4: **For** step $k = N - 1$ down to 0 **do**:
5: Calculate available resources $\mu_1(k)$ and $\mu_2(k)$ using Eq. (1)
6: Solve the local min-max optimization problem for the matrix game at step k
7: **If** condition Eq. (6) holds **then**:
8: Update preference set boundary: add valid states to $\Delta_1(k)$
9: Record optimal strategy $u^*(k)$ that satisfies the Bellman optimality principle
10: **Else**:
11: Game transitions to condition Eq. (3) or Eq. (4)
12: **End For**
13: **Return** accumulated set $\Delta_1(0)$

That is, for scenario 1, the defender's initial resources are $\mu_1(0) = 2.5$ and the attacker's are $\mu_2(0) = 3.2$. We substitute these values into Eq. (1) and obtain the following inequality— $5 \times \mu_1(0) + (4.3) \times \mu_2(0) \succ (6.7) \times \eta(0)$, which corresponds to the defender's terminal state.

The graph in Fig. 2 is a three-dimensional visualization of the preference set Δ_1 of the first player (the defender) in the problem of countering targeted ART attacks. The axes, respectively $\mu_1(0), \mu_2(0)$—the defender's initial financial resources allocated to two different defense strategies (in thousands of US dollars). And $\eta(0)$—the attacker's initial financial resources (in thousands of US dollars).

The planes in Fig. 2 (gray translucent surfaces) are the boundaries corresponding to individual inequalities from Table I. Given inequalities represent the results of the area of the first player's preference in countering targeted APT attacks modeling (in the context of finding the optimal strategy for allocating financial resources of the defense side to the means of IS).

Each plane divides the space into two parts—the region above the plane is part of the set Δ_1 for a given inequality. Since is the union of such half-spaces for all 15 inequalities, the final domain of the defender's preference is the union of the above-plane regions. The green dots satisfy at least one of the 15 inequalities, i.e., they belong to Δ_1. The red dots (one is shown, as many more were obtained during the game) do not satisfy any inequality, i.e., they are outside Δ_1. This representation clearly shows what combinations of initial financial resources will allow the defender to achieve his goal, i.e., prevent a successful ART attack, provided that the attacker acts rationally.

TABLE I. A FRAGMENT OF THE TABLE OF INITIAL DATA AND SIMULATION RESULTS

No	Initial Data for Modeling			Simulation Results
	$\mu_1(0)$	$\mu_2(0)$	$\eta(0)$	$\Delta_1(0)$
1	2.5	3.2	2.7	$5 \times \mu_1(0) + (4.3) \times \mu_2(0) \succ (6.7) \times \eta(0)$
2	10.1	1.3	5.2	$3 \times \mu_1(0) + (2.5) \times \mu_2(0) \succ (5.4) \times \eta(0)$
3	9.4	3.7	4.9	$\mu_1(0) + (8.3) \times \mu_2(0) \succ (1.7) \times \eta(0)$
4	6.9	8.0	4.3	$(1.3) \times \mu_1(0) + 2 \times \mu_2(0) \succ (5.7) \times \eta(0)$
5	7.4	3.8	1.1	$9 \times \mu_1(0) + (3.3) \times \mu_2(0) \succ (5.7) \times \eta(0)$
6	3.4	2.2	5.0	$3 \times \mu_1(0) + (2.3) \times \mu_2(0) \succ (0.7) \times \eta(0)$
7	9.6	1.8	3.2	$11 \times \mu_1(0) + (8.3) \times \mu_2(0) \succ 5 \times \eta(0)$
8	7.4	8.3	6.7	$2 \times \mu_1(0) + (9.3) \times \mu_2(0) \succ \eta(0)$
9	8.0	9.9	1.0	$14 \times \mu_1(0) + (8.3) \times \mu_2(0) \succ (7.7) \times \eta(0)$
10	5.1	2.0	7.4	$(3.9) \times \mu_1(0) + (4.3) \times \mu_2(0) \succ (2.7) \times \eta(0)$
11	3.8	7.6	3.0	$6 \times \mu_1(0) + (7.3) \times \mu_2(0) \succ (8.7) \times \eta(0)$
12	2.4	3.9	2.8	$15 \times \mu_1(0) + (1.3) \times \mu_2(0) \succ (9.7) \times \eta(0)$
13	9.0	5.6	2.9	$4 \times \mu_1(0) + (2.3) \times \mu_2(0) \succ \eta(0)$
14	3.7	8.0	1.8	$(0.3) \times \mu_1(0) + \mu_2(0) \succ \eta(0)$
15	2.1	4.3	1.1	$(7.3) \times \mu_1(0) + 2 \times \mu_2(0) \succ (11.2) \times \eta(0)$

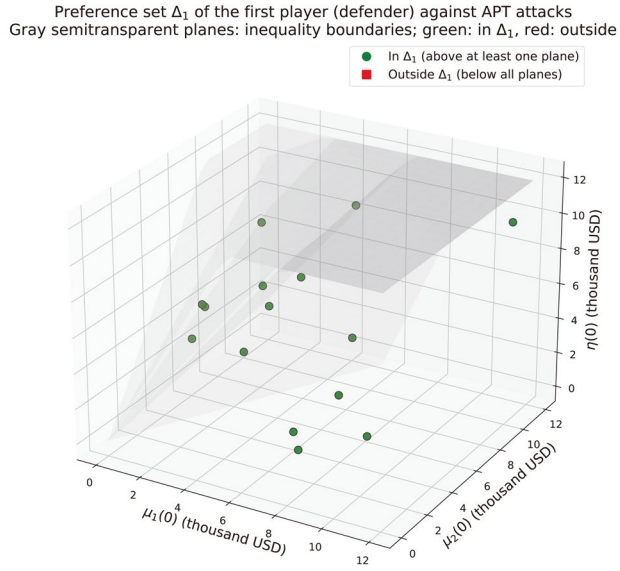

Fig. 2. Partial representation of the states of the preference set Δ_1 of the first player in the task of countering APT attacks for 3 variables in the test calculation.

Discussion of the results of a computational experiment

To objectively evaluate the effectiveness of the proposed multi-stage bilinear model, we compared it with a basic static approach to information security budget allocation. A classic one-stage zero-sum game was used as the baseline model. In this game, the defender (OI) allocates the initial budget $\mu_1(0)$ proportionally to the expected threats at the start. They have no ability to reallocate resources as the APT attack progresses.

For objective quantitative validation of the models, two key metrics are introduced. The first is the "Budget Survival Rate", i.e., the proportion of the defender's unspent funds when the game enters the terminal state. The second is the "Adversary Attrition Rate Index", i.e., the number of steps required to eliminate the attacker's budget. Evaluation using these metrics demonstrated the superiority of the proposed method. Thus, the bilinear strategy allowed the defense to preserve some of its reserves until the final phase of the confrontation. Meanwhile, the static and proportional distributions led to the complete exhaustion of the defender's financial resources, with the survival rate reaching zero, already in the early stages of the attack.

An analysis based on Scenario 1 data (Table I) revealed the following differences. Static model: With a rigid budget allocation, the defender is forced to spend resources on protecting all possible vectors at each stage k. In the context of a developing APT attack, this will lead to rapid budget depletion. In our simulation run of the static model, the defender exhausted its resources already at step $k = 3$. This led to the fulfillment of the terminal condition Eq. (3)—a successful compromise of the system, since the attacker still had the means to complete the attack. The bilinear model allowed for recalculation of the transformation matrices Φ_k and Ψ_k at each step. By applying Bellman's optimality principle, the defender invests only in those technological strategies that are relevant at the current stage of the attack. As a result, for the same Scenario 1, the defender was able to conserve some resources until the final stages (step $k = 5$) and bring the game to the terminal state Eq. (2)—the attacker's financial exhaustion while maintaining the operational capability of the OI.

A strategy for proportional distribution of the defense budget was implemented as an additional baseline method for comparison. With this strategy, the first player's total financial resources are allocated among K technological strategies at each step in proportion to the expected damage from the corresponding attacker strategies. Accordingly, the share of funds allocated to the j-th defensive strategy is equal to $\omega_j^1 / \sum_i \omega_i^1$, where ω_i^1 is the financial damage from the i-th attacker strategy, according to the matrix D_1. The strategy does not provide for dynamic reoptimization taking into account the matrices Φ_k and Ψ_k. The simulation results showed that the proportional strategy leads to depletion of defense resources already by step $k = 4$. The result is inferior to the proposed bilinear method. In the latter, the goal was achieved at step $k = 5$. However, it is somewhat superior to static distribution. The criteria for selecting the model parameters were based on real market data on the cost of APT attack components and security tools. Prices for exploits, malware writing, detection systems, sandboxes, etc., collected from open sources, were used. A sensitivity

analysis was conducted to assess the robustness of the solution.

To confirm the robustness and statistical significance of the proposed multivariate financial resource competition model, a series of stochastic simulations (1000 iterations) was conducted. The base costs of the attacker (C_A) and defender (C_A) were chosen as variable parameters with a normal noise distribution ($\sigma = 0.1$). Table II presents the calculated results of the main statistical descriptors for the model's output indicators: the defender's budget survival index (I_{SB}) and the attacker's resource leakage coefficient (K_{AL}).

TABLE II. STATISTICAL INDICATORS OF MODEL STABILITY IN STOCHASTIC MODELING

Metric	Expected Value	Dispersion	95% Confidence Interval (95% CI)
Survival index (I_{SB})	0.742	0.012	[0.721; 0.763]
Leakage coefficient (K_{AL})	0.315	0.008	[0.298; 0.332]

Narrow confidence intervals and low variance values confirmed that the proposed model retained convergence and predictive power even under conditions of changing funding levels of the parties.

The elements of the D_1 and D_2 matrices varied within a range of ±20%. In all variants, the optimal strategies retained their properties, and the terminal states did not extend beyond the preferred sets, confirming the robustness of the model.

It is imperative to acknowledge that any entity can become susceptible to APT attacks. The process of orchestrating an APT attack is both time-consuming and costly. However, its efficacy is notably high, particularly in the absence of reliable IS OI systems. As a case in point, we may consider the findings of APT attacks as outlined in the works of Smoliansky [31] and Kozhukhov [32]. As demonstrated previously, and as evidenced by data from open sources (e.g., proposals for orchestrating attacks on Internet forums, among others), we have ascertained the cost of services and specialized software utilized for the orchestration of various stages of APT attacks within the black market. These data were utilized during the computational experiment. Similarly, data concerning protection strategies against APT attacks were obtained from open sources [33]. Each strategy is associated with a specific cost. The financial implications of implementing a specific strategy in the realm of protection can be ascertained by consulting the pages of vendors specializing in the development of pertinent solutions. Consequently, computational experiments, grounded in the extant initial data, have enabled the identification of both sets of preferences and optimal financial strategies on the part of the defense side. However, this dynamic is equally applicable to the offensive side. The employment of an intelligent information system facilitated the visualization of the results of the game between the OI defender and the attacker, within the framework of analyzing the cost of defending and conducting an attack, respectively.

A notable limitation of the study is its failure to consider all potential variants of the game, encompassing both techniques and technologies for conducting APT attacks. The focal point of the study pertained to the confrontation between the offensive and defensive teams within the context of their financial resources, with the objective of attaining the players' objectives.

Unlike our previous studies [28, 34], which considered a general bilinear investment allocation scheme, this article describes a direct relationship between the choice of specific technological protection strategies, for example, the implementation of isolated software tools or monitoring systems, and their financial equivalent in the context of countering multi-stage APT attacks. For example, if a defender chooses a technological strategy j—deploying a \$2000 honeypot system, and an attacker chooses a strategy i—writing a unique exploit for \$3000, the elements of the D_1 and D_2 matrices will quantitatively reflect what portion of the attacker's budget will be offset by this defense. Ultimately, technological effectiveness directly translates into financial ratios.

The main contribution of this work is the introduction of the concept of "multivariant financial strategies." This concept is mathematically expressed through the variable restructuring of resource transformation matrices depending on the stage of an APT attack. This will allow the defender not only to estimate the budget but also to determine the terminal states at which the defense is guaranteed to achieve its goals.

We also note that solving the problem with complete information provides an effective tool for solving the problem with incomplete information in the process of studying APT attacks, both in the stochastic version and in the problem with fuzzy information.

It is imperative to acknowledge a significant constraint inherent in the proposed mathematical model. In the present version of the game, both players are assumed to possess complete information, including their respective financial resources and available strategies. In real-world APT attacks, the Defending Party (DFP) most often operates under conditions of severe uncertainty and information asymmetry, without knowing the attackers' exact budget.

It should be emphasized that using a full-information model allows us to obtain a lower bound for the required cybersecurity budget in a worst-case scenario. Unlike Bayesian games [35, 36], in which the defender has only probabilistic representations of the attacker's type and resources, or Stackelberg games [37, 38], in which the attacker acts with knowledge of the defensive strategy, a deterministic formulation with full information guarantees goal achievement under any adversary's permissible actions. As a result, the resulting solution provides a conservative estimate. That is, if the defender has sufficient resources to win under full information, then it will be even more likely to successfully defend itself under real-world conditions of uncertainty. This estimate serves as the foundation for a further transition to models with

incomplete information, where the resulting lower bounds will be used as basic constraints in constructing Bayesian or hierarchical strategies.

The latter is characteristic of Bayesian or Stackelberg games. However, the utilization of a full-information model at this stage is substantiated, as it facilitated the calculation of the "worst-case scenario" and the determination of mathematically rigorous lower bounds on the requisite information security budget for the IT facility. The subsequent logical progression will involve the transition to models with incomplete information, thereby facilitating the formulation of more flexible strategic recommendations.

The objective of this study is to consider the case for a multistep game with fuzzy information. It is this author's opinion that this is also an urgent task. It is imperative to acknowledge the limitation of the defense sector in comprehending the financial capacities of the adversary engaged in APT attacks.

To demonstrate the advantages of the developed multifactor model, a comparative quantitative simulation was also conducted under identical initial conditions. That is, with a fixed attack and defense budget, using two well-known game-theoretic approaches: the risk analysis model of Rass *et al.* [26] and the network economic model of Nagurney and Nagurney [15].

The comparison was conducted using two performance metrics. The first is the defender's budget survivability index I, where the optimal value tends to I_{SB}. The second is the attacker's financial resource leakage coefficient K_{AL}, which reflects the attacker's economic exhaustion, with the optimal value tending toward 1. The simulation results are presented in Table III.

TABLE III. COMPARISON OF THE MODELS EFFICIENCY IN A LONG-TERM TARGETED ATTACK (T = 50 STEPS)

Model	Budget Survival Index (BSI)	Attacker's Resource Leakage Rate (KAL)	Taking Into Account the Multifactorial Nature of Risks
Model Rass *et al.* [26]	0.58	0.18	Partial (static risks only)
Model Nagurney and Nagurney [15]	0.63	0.22	Partial (network streams only)
Proposed model	0.79	0.34	Full (dynamic financial factors)

As can be seen from Table III, the proposed multifactorial model provides a higher value of the budget survival index ($I_{SB} = 0.79$). This is 21–26% more effective than similar models. The latter is achieved through the flexible adjustment of defensive costs depending on the intensity of the attack. In addition, the attacker's resource leakage coefficient (K_{AL}) in our model was 0.34. This indicates a more rapid economic exhaustion of the attacking side compared to classical static models [15, 26]. As a result, the model [26] is focused primarily on the analysis of the equilibrium of the attacker and defender strategies. However, this model takes into account only a limited extent: depletion of the parties' budgets; redistribution of financial resources between attack stages; and the impact of long-term multi-stage APT scenarios.

Model of Nagurney and Nagurney [15] focuses primarily on assessing the economic efficiency of investments in cybersecurity. However, the model insufficiently considers: the attacker's behavior; changes in the cost structure during attack escalation; and the impact of multi-stage interactions between the parties.

Our model simultaneously considers: multi-stage conflict dynamics; bilinear resource distribution; changes in the financial status of the parties over time; adaptive budget redistribution; and the ability to analyze preferred sets of strategies.

V. CONCLUSION

A critical factor influencing the financial implications of an attack, particularly an APT attack, is the security level of an Information Security Object (ISO). Consequently, the absence of comprehensive and up-to-date information security measures significantly eases the operations of cybercriminals. From a defensive standpoint, it is imperative to comprehend the financial implications of APT attacks, both in terms of preparation and execution, in principle. The response to this inquiry will facilitate the formulation of a customized strategy for the allocation of resources to counteractions. This strategy will be informed by mathematical modeling techniques, which will be employed to optimize the utilization of FR for both APT attacks on the OI and for their protection. The authors propose a multifactorial model of countering targeted attacks within the framework of a bilinear multistep quality game with several terminal surfaces. The distinguishing feature of the model under consideration is its incorporation of multivariance, a term denoting the financial strategies employed by both defense and attack entities in their respective efforts to counter APT attacks. This multivariance is intricately woven into the dynamics of the interaction between these opposing sides, a feature that sets it apart from other models. This facilitates the consideration of the general problem of the formation of IS OI costs within the framework of the game scheme. This scheme can be used for the tasks of countering targeted attacks in the context of the distribution of finances of the parties to the game. A solution to the problem of countering targeted attacks was proposed; this solution was formulated as a bilinear multistep game of the quality of multidimensional objects. In the paper, the formulated problem was solved by employing the optimality principle of R. Bellman. In the context of this study, the solution was identified within the framework of a positional multistep game scheme with complete information. Preference sets and optimal financial strategies of the first player (defender against targeted attacks)-ally are determined. The necessary conditions are also given to guarantee the first defending player the opportunity to protect the OI in a finite time. The model described in the paper is implemented in the form of a software module for an intelligent information system. The computational

experiment, which was conducted in order to test the model's operability, was performed using the Anaconda distribution in the PyChar Professional programming environment. This made it possible to visualize the results of the game between the OI defender and the attacker, in the context of analyzing the cost of, respectively, defending and conducting an attack. The findings of the study are both scientifically novel and pertinent to the field. These results will be of use to information security analysts specializing in protecting various companies from APT attacks.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

V.M. and V.L.: Conceptualization; V.M., V.L. and B.A.: methodology; M.Y.: software; I.M. and Z.A.: validation; I.M.: formal analysis; V.M., V.L. and B.A.: investigation; B.A. and M.Y.: resources; I.M.: data curation; Z.A. and M.Y.: writing—review and editing; Z.A.: visualization; V.L.: supervision; B.A.: project administration; M.Y.: funding acquisition. All authors contributed to writing the manuscript, reviewed the final draft, and approved the final version.

FUNDING

The work was supported by a grant of the project of the GF "Zhas Galym" № AP 19174716 "Development of a decision support system based on Bayesian networks to improve the effectiveness of detecting intrusions into computer systems" and funding the Ministry of Science and Higher Education of the Republic of Kazakhstan and this work was partially supported by project No. 2.3/26-P of the National Academy of Sciences of Ukraine.

REFERENCES

[1] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Proc. Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference*, 2014, pp. 63–72.

[2] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[3] S. Dan. (May 2020). How much does it cost to launch a cyberattack? *CSO.* [Online]. Available: https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html

[4] J. Hua and S. Bapna, "The economic impact of cyber terrorism," *The Journal of Strategic Information Systems*, vol. 22, no. 2, pp. 175–186, 2013.

[5] J. Olech. (2022). The real costs of hacking a website (+ How to prevent it). *WizCase.* [Online]. Available: https://www.wizcase.com/blog/how-much-it-costs-to-hack-a-website/

[6] V. Lakhno, V. Malyukov, B. Akhmetov, D. Kasatkin, and L. Plyska, "Development of a model for choosing strategies for investing in information security," *Eastern European Journal of Corporate Technologies*, vol. 2, no. 3, 110. doi: 10.15587/1729-4061.2021.228313

[7] K. Staňková, J. S. Brown, W. S. Dalton, and R. A. Gatenby, "Optimizing cancer treatment using game theory: A review," *JAMA oncology*, vol. 5, no. 1, pp. 96–103, 2019.

[8] L. A. Gordon and M. P. Loeb "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[9] E. Panaousis, A. Fielder, P. Malacaria, C. Hankin, and F. Smeraldi, "Cybersecurity games and investments: A decision support approach," in *Proc. Decision and Game Theory for Security: 5th International Conference*, Los Angeles, 2014, pp. 266–286.

[10] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems*, vol. 86, pp. 13–23, 2016.

[11] N. G. Y. R. Douha, M. Sasabe, Y. Taenaka, and Y. Kadobayashi, "An evolutionary game theoretic analysis of cybersecurity investment strategies for smart-home users against cyberattacks," *Applied Sciences*, vol. 13, no. 7, 4645, 2023.

[12] H. Cavusoglu, S. Raghunathan, and W. T. Yue, "Decision-theoretic and game-theoretic approaches to IT security investment," *Journal of Management Information Systems*, vol. 25, no. 2, pp. 281–304, 2008.

[13] A. Sood and R. Enbody, *Targeted Cyber Attacks: Multi-Staged Attacks Driven by Exploits and Malware*, Syngress, 2014.

[14] G. Bunker, "Targeted cyber attacks: How to mitigate the increasing risk," *Network Security*, vol. 2020, no. 1, pp. 17–19, 2020.

[15] A. Nagurney and L. S. Nagurney, "A game theory model of cybersecurity investments with information asymmetry," *NETNOMICS: Economic Research and Electronic Networking*, vol. 16, pp. 127–148, 2015.

[16] A. Nagurney, L. S. Nagurney, and S. Shukla, "A supply chain game theory framework for cybersecurity investments under network vulnerability," *Computation, Cryptography, and Network Security*, pp. 381–398, 2015.

[17] A. Nagurney, P. Daniele, and S. Shukla, "A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints," *Annals of Operations Research,* vol. 248, pp. 405–427, 2017.

[18] D. K. Tosh, I. Vakilinia, S. Shetty, S. Sengupta, C. A. Kamhoua, L. Njilla, and K. Kwiat, "Three layer game theoretic decision framework for cyber-investment and cyber-insurance," in *Proc. Decision and Game Theory for Security: 8th International Conference, GameSec 2017*, Vienna, 2017, pp. 519–532.

[19] B. Hyder and M. Govindarasu, "Optimization of cybersecurity investment strategies in the smart grid using game-theory," in *Proc. 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT),* 2020, pp. 1–5.

[20] W. Sun, X. Kong, D. He, and X. You, "Information security problem research based on game theory," in *Proc. 2008 International Symposium on Electronic Commerce and Security*, 2008, pp. 554–557.

[21] N. Y. R. Douha, B. O. Sane, M. Sasabe, D. Fall, Y. Taenaka, and Y. Kadobayashi, "Cost-benefit analysis toward designing efficient education programs for household security," in *Proc. The Fifteenth International Conference on Emerging Security Information, Systems and Technologies, IARIA SECURWARE*, Athens, 2021, pp. 14–18.

[22] J. Grossklags, N. Christin, and J. Chuang, "Secure or insure? A game-theoretic analysis of information security games," in *Proc. the 17th International Conference on World Wide Web*, 2008, pp. 209–218.

[23] S. Musman and A. Turner, "A game theoretic approach to cyber security risk management," *The Journal of Defense Modeling and Simulation*, vol. 15, no. 2, pp. 127–146, 2018.

[24] D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe, "Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness," *Journal of Artificial Intelligence Research*, vol. 41, pp. 297–327, 2011.

[25] B. Srinidhi, J. Yan, and G. K. Tayi, "Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors," *Decision Support Systems*, vol. 75, pp. 49–62, 2015.

[26] S. Rass, S. König, and S. Schauer, "Defending against advanced persistent threats using game-theory," *PloS one*, vol. 12, no. 1, e0168675, 2017.

[27] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, "A survey of game theoretic methods for cyber security," in *Proc. 2016 IEEE First International Conference on Data Science in Cyberspace (DSC),* 2016, pp. 631–636.

[28] B. Akhmetov, V. Lakhno, V. Malyukov, B. Akhmetov, B. Yagaliyeva, M. Lakhno, and Y. A. Gulmira, "Model for managing the procedure of continuous mutual financial investment in cybersecurity for the case with fuzzy information," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 93, pp. 539–553, 2022.
[29] F. Wehinger, "The dark net: Self-regulation dynamics of illegal online markets for identities and related services," in *Proc. 2011 European Intelligence and Security Informatics Conference,* 2011, pp. 209–213.
[30] V. P. Malyukov, "Game of quality for two groups of objects," *Cybernetics*, vol. 26, pp. 698–710, 1990.
[31] M. Smoliansky. (2020). How to defend against advanced persistent threats. *Deep Instinct.* [Online]. Available: https://www.deepinstinct.com/blog/how-to-defend-against-advanced-persistent-threats
[32] Dmitry Kozhukhov. (2020). What is an APT attack and how to protect yourself from it? [Online]. Available: https://spy-soft.net/apt-attack/
[33] G. D. Maayan. (Mar 2023). Advanced Persistent Threat Security: 5 Modern Strategies. *IEEE Computer Society*. [Online]. Available: https://www.computer.org/publications/tech-news/trends/strategies-for-apt-defense
[34] L. Valeriy, M. Volodymyr, K Olena, T. Mykola, D. Alyona, and M. Tetyana, "Model of evaluating smart city projects by groups of investors using a multifactorial approach," *Communications in Computer and Information Science*, pp. 13–26, 2020. doi: 10.1007/978-3-030-42517-3_2
[35] D. Lappas, P. Karampelas, and G. Fesakis, "Enhancement of phishing email detection with bayesian networks: A cyber security training module," in *Proc. European Conference on Cyber Warfare and Security,* 2025, pp. 328–337.
[36] M. J. Pappaterra and F. Flammini, "A review of intelligent cybersecurity with Bayesian networks," in *Proc. 2019 IEEE International Conference on Systems, Man and Cybernetics* (SMC), 2019, pp. 445–452.
[37] Y. Zhang and P. Malacaria, "Bayesian stackelberg games for cyber-security decision support," *Decision Support Systems*, vol. 148, 113599, 2021.
[38] A. A. Temghart, M. Marwan, and M. Baslam, "Stackelberg security game for optimizing cybersecurity decisions in cloud computing," *Security and Communication Networks*, vol. 2023, no. 1, 2811038, 2023.