Strategy for Countering Phishing Attacks within the Endless Antagonistic Game Framework

Valery Lakhno [1], Volodimir Malyukov [1], Inna Malyukova [2], Bakhytzhan Akhmetov [3], Zhuldyz Alimseitova [4,*], and Atkeldi Ogan [4]

[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, Institute of Automation and Information Technologies, Satbayev University, Almaty, Kazakhstan
Email: lva964@nubip.edu.ua (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.); atkeldi@mail.ru (A.O.)
*Corresponding author

***Abstract*—A mathematical model has been developed for the computational core of the decision support system taken in the course of ensuring information security of exchange sessions for the sale and purchase of digital cryptocurrencies. The model contributes to making rational decisions to ensure the information security of players who may face the threat of phishing attacks against them. The model was developed on the basis of an infinite antagonistic game and is designed to find the optimal strategies for players. The solution of such a problem contributes to the analytical search not only for the value of the game, but also makes it possible to find the characteristics of the risk degree of achieving the goal by the players when they use optimal mixed strategies. The described solution contributes to the analysis of the situation with counteraction to the party attacking with the help of phishing the participant of the trading session for buying and selling digital cryptocurrencies. Computational experiments were carried out using the Anaconda distribution kit. The results obtained will be useful for analysts dealing with information security issues of trading platforms, specializing in the purchase and sale of digital cryptocurrencies, and counteracting the threats phishing attacks. During research, three specific zones in the resource space have been identified: "Safe Zone", "Strategic Parity Zone", and "Critical Risk Zone". Mathematically proven, the "Safe Zone" of cryptocurrency exchange is not constant. It deforms nonlinearly as market trends change. The obtained results give informational security analysts a tool for the flexible redistribution of defense budgets during periods of high market volatility.**

***Keywords*—endless antagonistic game, optimal strategy, phishing attack, trading session, digital cryptocurrency**

I. Introduction

As the scale of the use of various Internet technologies develops, the number of cyber threats, as well as all kinds of attacks aimed at computer systems, also increases. Computer intruders not only invent new methods and scenarios for conducting cyber-attacks, but also improve old proven schemes. For example, despite the rapid development of various intrusion detection systems, the threat of phishing, which occupies a significant share among computer attacks, has not disappeared. These attacks make it possible for cybercriminals to steal user account data from various Internet sites. At the same time, attackers do not particularly bother developing new scenarios for conducting a phishing attack [1]. And, indeed, phishing methods such as sending fake emails, spoofing websites, etc., are still effective for attackers.

Phishing has not bypassed such a popular type of commercial activity in recent years as trading in Digital Cryptocurrencies (DCC) and, accordingly, has affected online exchanges involved in such transactions. With the development and growth of the popularity of exchanges involved in trading DCC, the problem of detecting and predicting the consequences of such attacks, including those based on phishing, still remains relevant. In Ref. [1], examples of a number of fraudulent attacks aimed at DCC exchanges are considered. Information Security (IS) professionals are looking for ways to ensure the cooperation of all stakeholders in order to counter fraud using phishing attack techniques and increase privacy for individuals and businesses. However, many issues still need to be studied in more detail, in particular, based on game-theoretic methods for analyzing situations that may arise as a result of a phishing attack. For example, when such an attack is aimed at clients of trading platforms involved in the purchase and sale of

Manuscript received February 22, 2026; revised April 15, 2026; accepted May 6, 2026; published July 23, 2026.

DCC. That is why in this publication we have tried to present our vision of this issue.

To construct an adequate mathematical model, we formalize the interaction between the attacker and the exchange not as a static process, but as a dynamic game with variable strategies. Overall, we can identify six main scenarios, which we will examine through the lens of game theory.

Strategy 1: "Mass Phishing—Targeted Attack". In this game, the attacker chooses between the "low cost—wide reach" and "high cost—high conversion" strategies. Note that mass phishing is characterized by minimal attack costs. These include spam mailings and cloning low-quality interfaces. And here the attacker's advantage is determined by the law of large numbers, despite the low probability of success p per user. Exchange protection here is built on basic filtering (Sender Policy Framework (SPF)/DomainKeys Identified Mail (DKIM)) and notifications. Or a targeted attack on Very Important Person (VIP) clients, which is an inverted strategy. That is, high investment in quality. This includes branding, purchasing drops, Search Engine Optimization (SEO), and more. Here, the attacker maximizes the potential gain V from a single incident, such as compromising "whales," while accepting the risk of high sunk costs in the event of failure.

Strategy 2: Social engineering attacks. This scenario introduces an element of interactivity into the game. The attacker simulates interaction with customer support. This transforms the game from a static one to a multi-step one. Success depends not only on technical means but also on the "human factor." However, this will require the model to take into account probabilistic parameters of user trust.

Strategy 3: Time synchronization with market volatility. In this case, phishing effectiveness correlates with market cycles. During periods of high volatility, i.e., "pumps" or panics, the cognitive load on users increases. This increases the likelihood of error and the success of a phishing attack. For the exchange, this means the need for flexible management of the security budget. In other words, increased monitoring costs occur precisely during peak periods of load on the cryptocurrency exchange.

Strategy 4: Consider the nonlinearity of damage and reputation. In traditional phishing models, damage is linear. However, in the Context of Crypto Exchanges (CEX), reputational losses are either threshold or cumulative. A single successful attack involving a large amount can trigger a liquidity outflow. And this outflow is disproportionate to the CEX's direct losses. This forces the exchange to choose strategies that minimize not only the expected value of losses but also the maximum possible risk.

Strategy 5: Evolutionary "Arms Race" between the attacker and CEX. The interaction in this case is like an endless game. Each iteration leads to a reconfiguration of both parties' strategies. The exchange's investment in detection, for example, based on machine learning, forces the attacker to improve the quality, i.e., the realism, of their websites. This will raise the barrier to entry for attackers, but does not completely eliminate the threat.

Strategy 6: Third-party introduction. Or risk insurance. If full protection is not possible, CEX can hedge risks through cyber insurance instruments. This transforms the zero-sum game between two parties into a system where some of the risk is transferred to an external player, i.e., the insurer. The latter modifies the exchange's utility function U_D by converting stochastic losses into deterministic operating costs, or the so-called insurance premium.

The mathematical model presented below is aimed at solving the practical problem of resource management in the context of a continuous "arms race" between cryptocurrency exchanges and attackers. Given the multi-stage and dynamic nature of modern attacks, the proposed mathematical apparatus serves as an analytical tool for Information Security Officers (ISOs). It will allow making informed decisions on the prompt redistribution of budgets between preventive protection and monitoring mechanisms in a synchronous manner. The latter is relevant during peak load periods on cryptocurrency exchange information security systems.

The listed strategies—of the exchange attacker and the exchange itself, as players opposing each other–can be considered part of the set of possible player choices. Given that the set of strategies increases over time, it makes sense to translate this circumstance into the assumption that players are entitled to consider themselves able to choose their strategy implementations from an infinite set of strategy values. Then the process of conflict interaction between the parties can be represented as an infinite antagonistic game, and the process of dominance used to find optimal mixed strategies can be considered a method for finding the carrier of optimal mixed strategies, in particular, such as the above six strategies. It should be noted that the use of optimal mixed strategies in a conflict depends on the ratio of the financial resources of the parties and other parameters that determine the interaction, and, consequently, the frequency of application of its most important variable strategies, which corresponds to the optimal mixed strategies of the players, also depends on this.

The mathematical model presented below is intended to describe one of the given scenarios, and it is within the framework of this article that the scenario of finding optimal mixed strategies that allow finding an acceptable result of conflict interactions attacking the exchange and the exchange itself as a defender from an attack on exchange participants is described. And, accordingly, find the optimal strategy for allocating resources between preventative protection, monitoring, and compensation mechanisms for a given scenario. It should be noted that in this article, we are only considering a defense strategy against an attack on the exchange. The attacker's strategy is found similarly. Therefore, the process for finding it will not be described.

The formulation of the six strategies presented above is derived from recent empirical observations and theoretical concepts in the field of cryptocurrency security. In particular, the dynamics of mass and spear

phishing (Strategy 1) and social engineering (Strategy 2) are based on established models of adversarial classification. The relationship between attack effectiveness and market volatility (Strategy 3), along with nonlinear reputational damage in decentralized finance (Strategy 4), is substantiated by recent research on cryptocurrency exchange risks, which are discussed in the next section of the article. Furthermore, the conceptualization of a continuous "arms race" (Strategy 5) and risk mitigation through third-party insurance (Strategy 6) directly extend evolutionary game models discussed in the modern literature, which is reviewed below.

The solution involves the apparatus of game theory, which made it possible to mathematically consider the situation with the counteraction of the party attacking the participant of the trading session for buying and selling DCC with the help of phishing.

II. Analysis of Previous Studies

Considering the retrospective of the development of the DCC market, as well as the corresponding cryptocurrency exchanges (hereinafter referred to as CCE), we can see that interest in this market is growing rapidly over a relatively short period of time. In particular, only in recent years, dozens of publications have appeared on the activities of such barges and the problems of modeling their activities [2–6].

It is shown that CCE facilitate trading between private investors and individual companies that recognize DCC as legitimate means of payment [6–8]. We can talk about a certain analogy between the classical exchange activity and the activity of exchanges dealing with transactions with DCC [8].

It is shown that the status of information security on cryptocurrency exchanges can only be improved by introducing stricter supervision and information security control mechanisms for trading platforms and their electronic services, which necessitates further research [9–11].

The first facts related to the hacking the CCE were recorded already at the opening of the first trading platforms. One of the most high-profile was the hacking of the MtGox exchange (Japoria) in 2011. This case was widely covered in the scientific press [12, 13]. Although the fact of hacking was recorded, no proper conclusions were drawn [14, 15].

In 2016, the Bitfinex exchange in the US was hacked. The hack led to the collapse of the Bitcoin exchange rate [16, 17]. In fact, this is the second case when a direct hack of trading services had a direct impact on the course of the DCC. The seriousness of the situation was evidenced by the fact that the US FBI specialists joined the investigation.

With the appearance of Blockchain, hackers have refocused their attack and hacking techniques in a new way. So, for example, ransomware viruses, Trojans, principles of using fake sites were redesigned for Blockchain, i.e., phishing [18].

Phishing attacks aimed at exchanges, digital services and players involved in DCC trading are still relevant. Phishing attacks are fraught with threats associated with the leakage of users' personal data. One example of such a leak was the case when a hardware platform for supporting crypto wallets Ledger (France) leaked data relating to more than 270,000 crypto wallets [19]. Such leaks may not immediately bring dividends to attackers, but they contribute to the fact that some of the information can be used by hackers in further attacks. We note that not all phishing attacks bring results for the attacking side. After all, users have become much more scrupulous about new links. And often such attacks go without consequences. Much more dangerous are attacks on financial digital services (crypto-exchanges) associated with the DCC.

The most serious risks are associated with a 51% attack. Although for attackers such an attack is associated with the risks of losing their own financial investments in its implementation. This type of attack is the costliest for attackers, since attackers need to incur significant expenses for the purchase (rent) of equipment. Note that a 51% attack is typical for blockchains that operate in accordance with the Proof-of-Work algorithm. While in the case of Bitcoin (BTC) it would be almost impossible for an attacker to obtain an amount of computing power that would exceed the rest of the network, this is quite feasible for small DCC. So, for example, compared to BTC, altcoins (Near, Polkadot, TWT, Doge, Monero, Luna, etc.) are characterized by a fairly low hashrate to protect the blockchain. Therefore, 51% attacks can indeed occur in their network [20].

Despite all the above, such attacks are not uncommon. For example, in 2018, such an attack was recorded, during which ZenCash DCC was attacked. During the attack, double expenses amounted to 550 thousand US dollars, and the costs were about 33 thousand US dollars. Similar attacks were recorded on Verge, BitcoinGold and Electroneum [21].

Many potential attacks on the DCC market are only hypothetically possible, since their implementation requires large resources from the cracker. However, traditional attacks, such as DDOS and phishing attacks, can cause DCC rates to fluctuate. And this, in turn, can be used in forex, where you can open short positions, quickly reverse transactions and hedge risks. And one effective attack for the attackers is enough for the DCC to become cheaper. A vivid example is Mt.Gox, when the attackers managed to quietly withdraw 650,000 BTC from the exchange.

In addition to hacking the CCE, attackers often began to use social engineering methods [22]. This often pays off, especially when cybercriminals are confronted by an emerging player in the DCC market.

It is quite difficult to defend against such attacks, and the most reliable way is to increase the literacy of market players and the usual vigilance when performing transactions with DCC.

The number of attacks directed at CCE is likely to increase, since attackers in the course of implementing a

successful attack can receive a fairly large reward [23, 24].

It should be noted that the leading companies in the field of cybersecurity have only just begun to form for themselves a new landscape of cyber threats related to the activities of the CCE. And the creators of the CCE are not yet fully ready to invest in the CCE, IS, preferring quick profits from transactions with the DCC.

Spear phishing on CCE is a type of cyber-attack in which attackers send hyperlinks, for example, using email, to well-researched targets [24, 25]. The purpose of such attacks is to obtain sensitive information by imitating trusted websites. However, in many models described in the scientific literature, in particular [26–31], there are no aspects that affect the analysis of the participants' choice of strategies for the actions of players in the DCC market. In our opinion, in order to solve this problem, a game-theoretic approach is needed to understand the point of view of an attacker (hacker) and a "victim" who can interact within the trading sessions on the CCE.

All of the above predetermines the relevance of new research in the direction of developing new methods and models for assessing the information security of the DCC market.

In addition to classic attack vectors, recent research has highlighted the growing threat of AI-driven phishing, including the use of deepfakes and the automated generation of targeted messages [32–36]. The development of generative AI has significantly lowered the barrier to entry for sophisticated social engineering attacks, making them scalable and difficult to detect [37–40]. These studies have confirmed the relevance of Strategy 5, which we described, viewing the attacker-victim interaction as an endless game in which attackers continuously increase the realism of phishing sites in response to improvements in exchange's detection systems.

The analysis of publications devoted to the issues of information security in the DCC market showed that the success and profitability for the transaction investor is largely determined by the understanding and attitude to potential risks, including those associated with the information security of exchange services. This aspect of the study of issues related to the DCC is of particular interest in the context of the objectives of the study. And, accordingly, it deserves a comprehensive study in the framework of the current study.

III. Purpose and Objectives of the Study

The purpose of the work is the development of mathematical models that form the computational core of the decision support system made during the trading session of the exchange for the sale and purchase of DCC and aimed at providing information security to players who may face the threat of a phishing attack against them.

During the study, the following tasks were solved:

- Development of a model on the basis of game theory (an infinite antagonistic game) for finding optimal strategies for players. That will make it possible to analytically find the value of the game and the characteristics of the risk degree of achieving the goal by the players when they use optimal mixed strategies. In particular, such a solution contributes to the analysis of the situation with counteraction to a party attacking, using phishing, a participant in a trading session for buying and selling DCC.
- Quantitative assessment of nonlinear deformation of crypto exchange security boundaries under market stress and volatility using computational simulations in Python.

IV. Materials and Methods

This paper formulates the problem statement for mitigating phishing attacks, wherein malicious actors target legitimate DCC trading participants with the intent of causing financial and operational harm. We will call these parties as players. The first player is a participant in the trading session for buying and selling DCC (in other words, a victim who suffered from the consequences of a phishing attack). The second player is an attacker who seeks to inflict damage through phishing.

The first player has M strategies, such as accepting false information, partially ignoring it, avoiding it, and others. The second player has N strategies, including the following: using email to conduct phishing campaigns, social engineering, using fake sites, using software bookmarks, and others.

As you know, any strategy of the player-intruder leads to financial losses for the victim. Let the intruder apply his i–strategy in the established financial system for the purchase and sale of the DCC. The use of this strategy brings financial damage δ_i . Further, let the player-victim apply his j –strategy in the established financial system for buying and selling DCC. The application of this strategy brings financial additions σ_j. Denote s_{ij}^1 by relation δ_i/σ_j, and s_{ij}^2 by relation σ_j/δ_i. If $\delta_i = 0$ for some i or $\sigma_j = 0$ for some$j$, then we exclude such strategies from consideration. The first player, having at the moment of time $t = 0$ $x(0)$ financial resources (hereinafter FinR) increases (or reduces) them to the value $g_1 \times x(0)$ of resources (g_1–the growth rate of FinR of the first player–the victim). Then he determines the amount of his investment $u(0) \times g_1 \times x(0)$, by choosing $u(0)$: $0 \le u(0) \le 1$. It is assumed that he is given the structure of investing his strategies, which is given by the set: $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_M$: $0 \le \alpha_i \le 1, \sum_{i=1}^{M} \alpha_i = 1$. Here M is the number of strategies of the first player. That is, the value of the investment can be written as follows:

$$u(0) \times g_1 \times x(0 = \alpha_1 \times u(0) \times g_1 \times x(0) + \ldots + \alpha_M \times u(0) \times g_1 \times x(0).$$

The value $\alpha_1 \times u(0) \times g_1 \times x(0)$ compensates $\sum_{i=1}^{N} s_{i1}^1 \times \alpha_1 \times u(0) \times g_1 \times x(0)$ of losses from the actions of an attacker. This will be expressed in the fact that the FinR of the attacking player will decrease by this

amount. The value $\alpha_j \times u(0) \times g_1 \times x(0), j = 1,\dots,M$ compensates $\sum_{i=1}^{N} s_{ij}^1 \times \alpha_j \times u(0) \times g_1 \times x(0)$ of losses from the actions of an attacker. This will be expressed in the fact that the FinR of the attacking player will decrease by this amount. That is, the total compensation for losses from the second player from the investment of the first player is equal to: $\sum_{j=1}^{M}\sum_{i=1}^{N} s_{ij}^1 \times \alpha_j \times u(0) \times g_1 \times x(0)$.

Let denote, by r_1 the coefficient $\sum_{j=1}^{M}\sum_{i=1}^{N} s_{ij}^1 \times \alpha_j$. The second player, having at the time $t = 0 y(0)$ of FinR increases them (or reduces them) to the value $g_2 \times y(0)$ of resources (g_2–the growth rate of FinR of the first player–the victim). He then determines the value of his investment $v(0) \times g_2 \times y(0)$ by choosing $v(0): 0 \le v(0) \le 1$.

It is assumed that the structure of investment by him of his strategies is given, which is given by the set: $\beta_1, \beta_2, \beta_3. \beta_4, \dots \beta_N: 0 \le \beta_i \le 1, \sum_{i=1}^{N} \beta_i = 1$. Here N–the number of strategies of the second player, i.e. the amount of investment can be written as: $v(0) \times g_2 \times y(0) = \beta_1 \times v(0) \times g_2 \times y(0) + \dots + \beta_N \times v(0) \times g_2 \times y(0)$.

The value $\beta_1 \times v(0) \times g_2 \times y(0)$ levels out $\sum_{j=1}^{M} s_{1j}^2 \times \beta_1 \times v(0) \times g_2 \times y(0)$ of income from the actions of the first player–victim. This will be expressed in the fact that the FinR of the player-victim will decrease by this amount. The value $\beta_i \times v(0) \times g_2 \times y(0), i = 1,\dots,N$ levels out $\sum_{j=1}^{M} s_{ij}^2 \times \beta_i \times v(0) \times g_2 \times y(0)$ of income from the actions of the first player–victim. This will be expressed in the fact that the FinR of the player-victim will decrease by this amount. That is, the total leveling of the FinR of the first player-victim from the investments of the second player-attacker is equal to:

$$\sum_{j=1}^{N}\sum_{i=1}^{M} s_{ij}^2 \times \beta_i \times v(0) \times g_2 \times y(0).$$

Let denote, by r_2 the coefficient:

$$\sum_{j=1}^{N}\sum_{i=1}^{M} s_{ij}^2 \times \beta_i \times \gamma_k = \frac{1+\dots+(r_1 \times r_2)^k}{1+\dots(r_1 \times r_2)^{k-1}}, k = 1,\dots, \gamma_1 = [1 + (r_1 \times r_2)]$$

Then the FinR of the players at the moment of time $t = 1$ can be written as follows:

$$x(1) = g_1(1 - u(0))x(0) - r_2 g_2 v(0) y(0),$$
$$y(1) = g_2(1 - v(0))y(0) - r_1 g_1 u(0) x(0),$$

There are 4 possible cases at the moment of time $t = 1$:

$$(1)\ x(1) \ge 0, y(1) < 0;$$
$$(2)\ x(1) < 0, y(1) \ge 0;$$
$$(3)\ x(1) \ge 0, y(1) \ge 0;$$
$$(4)\ x(1) < 0, y(1) < 0;$$

The first case is desirable for the first player.

The second case is desirable for the second player.

The third and fourth cases are neutral for the players, i.e. for both players they are not a priority. Players are not interested in the possibility of further interaction in time; their goals are to achieve the desired results for them already at the moment of time $t = 1$. This means that they tend to choose their investment strategies in order to achieve their goals. To do this, they need to solve an infinite antagonistic game in normal form, which is formalized as follows. Let denote by U and V the unit segment $[0,1]$, and by K the function on $U \times V$ with values in R:

$$K = \begin{cases} +1, & x(u,v) \ge 0,\ y(u,v) < 0; \\ -1, & x(u,v) < 0,\ y(u,v) \ge 0; \\ 0, & \text{otherwise.} \end{cases}$$

Then the infinite antagonistic game will be written as follows: $\Gamma = < U, V, K >$. In the game under consideration, there are no optimal pure strategies, but there are game values v^* and optimal mixed strategies. Let's describe them.

Let denote:

$$\gamma_k = \frac{1+\dots+(r_1 \times r_2)^k}{1+\dots(r_1 \times r_2)^{k-1}}, k = 1,\dots, \gamma_1 = [1 + (r_1 \times r_2)].$$

In the case $r_1 \times r_2 < 1$ we have:

$$v^* = \begin{cases} -1, y(0) \ge 0, r_2 \times g_2 \times y(0) \succ (1 + r_1 \times r_2) \times g_1 \times x(0), \\ -\frac{1}{2}, y(0) \ge 0, r_2 \times g_2 \times y(0) \le [1 + r_1 \times r_2] \times g_1 \times x(0), r_2 \times g_2 \times y(0) \succ \gamma_2 \times g_1 \times x(0), \\ -\frac{1}{k}, y(0) \ge 0, r_2 \times g_2 \times y(0) \le \gamma_{k-1} \times g_1 \times x(0), r_2 \times g_2 \times y(0) \succ \gamma_k \times g_1 \times x(0), \\ 0, x(0) \ge 0, r_2 \times g_2 \times y(0) \le g_1 \times x(0), g_2 \times y(0) \ge r_1 \times g_1 \times x(0), \\ \frac{1}{k}, x(0) \ge 0, g_2 \cdot y(0) \ge \frac{1}{\gamma_{k-1}} \times g_1 \times r_1 \times x(0), g_2 \times y(0) \prec \frac{1}{\gamma_k} \times g_1 \times r_1 \times x(0), \\ \frac{1}{2}, g_2 \times y(0) \ge \frac{1}{\gamma_1} \times r_1 \times g_1 \times x(0), g_2 \times y(0) \succ \frac{1}{\gamma_2} \times r_1 \times g_1 \times x(0), \\ 1,\ x(0) \ge 0, g_2 \times y(0) \prec \frac{1}{\gamma_1} \times r_1 \times g_1 \times x(0), \\ 0, x(0) \prec 0, y(0) \prec 0; \end{cases} \quad (1)$$

It is obvious that the procedure for finding zones is designed in such a way that the "piecewise" conditions guarantee that the different regions do not mathematically overlap and are complete. Moreover, it follows from the problem statement that the mathematical expressions in Eq. (1) are clearly defined, and the boundary conditions are determined by the problem statement and are correct.

In the case $r_1 \times r_2 \geq 1$ the record for the game value differs only in the record of the area in the players' FinR space, in which $v^* = 0$. This area will be written as follows:

$$y(0) \geq 0, r_1 \times g_1 \times x(0) \geq g_2 \times y(0),\ r_2 \times g_2 \times y(0) \geq g_1 \times x(0) \quad (2)$$

The optimal mixed strategies of the players will be probability measures with carriers consisting of a finite number of points. Moreover, if the value of the game is $\pm\frac{1}{k}$, then the carrier of such probability measures has k points. At points, the value of the probability measure of each player is $\frac{1}{k}$.

Let us give a notation for the carrier points of these probability measures in the case when the value of the game is positive. If the value of the game is equal to $\frac{1}{k}$, then the record of the carrier points of optimal mixed strategies is as follows:

$$u_1^* = 1 - \frac{r_2 \times g_2 \times y(0)}{g_1 \times x(0)}, v_1^* = 1,$$
$$u_2^* = [1 + r_1 \times r_2] \times \left[1 - \frac{r_2 \times g_2 \times y(0)}{g_1 \times x(0)}\right],$$
$$v_2^* = (1 + r_1 \times r_2) - \frac{r_1 \times g_1 \times x(0)}{g_2 \times y(0)}$$
$$u_k^* = [1 + \cdots + (r_1 \times r_2)^{k-1}] \times [1 - \frac{\left(r_2 \times g_2 \times y(0)\right)}{\left(g_1 \times x(0)\right)}],$$
$$v_k^* = [1+\ldots+(r_1 \times r_2)^{k-1}] - [1+\ldots+(r_1 \times r_2)^{k-2}] \times \frac{r_1 \times g_1 \times x(0)}{g_2 \times y(0)}, k \geq 3 \quad (3)$$

If the value of the game is negative, then the notation for the carrier points of optimal mixed strategies is symmetric. Namely, it is necessary to change the index 1 to 2 and the variables $x(0)$ to $y(0)$, u_k^* to v_k^*.

In the case when $v^* = 0$ there are optimal pure strategies. At

$$r_1 \times r_2 \prec 1, g_1 \times x(0) \geq r_2 \times g_2 \times y(0), g_2 \times y(0) \geq r_1 \times g_1 \times x(0),$$
$$u_1^* = \frac{1}{(1 - r_1 \times r_2)} \times [1 - \frac{\left(r_2 \times g_2 \times y(0)\right)}{\left(g_1 \times x(0)\right)}],$$
$$v_1^* = \frac{\left(g_1 \times x(0)\right)}{\left(g_1 \times x(0)\right)} \times \{1 - \frac{1}{1 - r_1 \times r_2} \times [1 - \frac{r_2 \times g_2 \times y(0)}{g_1 \times x(0)}]\} \quad (4)$$

Optimal pure strategies are defined in the same way and at

$$r_1 \times r_2 > 1, r_1 \times g_1 \times x(0) \geq g_2 \times y(0),\ r_2 \times g_2 \times y(0) \geq r_1 \times g_1 \times x(0). \quad (5)$$

At $r_1 \times r_2 = 1$ the optimal pure strategies of the players are $u_1^* = 0, v_1^* = 0$.

Thus, the value of the considered infinite antagonistic game and the optimal strategies of the players are found. In essence, the absolute value of the game characterizes the risk degree of achieving the goal by the players when they use optimal mixed strategies.

To visualize the logic of the proposed game-theoretic model, a structural block diagram of the system is shown in Fig. 1. It illustrates the integration of input data, such as market trends and performance metrics, with the model's computational core. This ultimately enables the information security analyst to select the optimal hybrid security investment strategy.

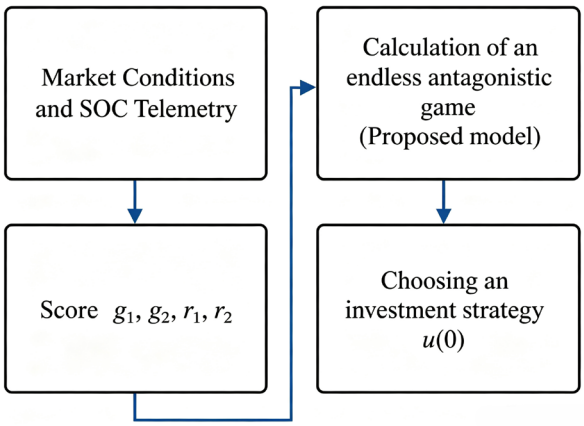

Fig. 1. Scheme of the logic of the proposed game-theoretic model.

To ensure absolute clarity regarding the mathematical apparatus used in this study, all key symbols, variables and operators used in the model are defined in Table I.

For practical application of the proposed model in real trading systems, an information security analyst needs to calibrate the investment efficiency coefficients r_1 and r_2.

In crypto exchange practice, these parameters are extracted from telemetry data from Security Operations Centers (SOCs) and SIEM systems. The protection ratio r_1 can be empirically calculated as the ratio of the prevented damage to the cost of implementing and maintaining specific countermeasures. Such countermeasures include the ML filtering system for the reporting period. The attack effectiveness ratio r_2, on the other hand, is estimated based on historical threat intelligence. In other words, it is the ratio of the average potential damage from a successful compromise, taking into account the law of large numbers, to the attacker's estimated operational costs, such as the cost of spamming, phishing, or infrastructure rental.

TABLE I. GLOSSARY OF MATHEMATICAL SYMBOLS AND OPERATORS

Symbol	Definition
M, N	Total number of available strategies for the first player (exchange/victim) and the second player (attacker), respectively.
δ_i	Financial damage inflicted by the attacker's i-th strategy.
σ_j	Financial additions (benefits) generated by the exchange's j-th strategy.
s_{ij}^1	Ratio of financial damage to financial additions (δ_i/σ_j).
s_{ij}^2	Ratio of financial additions to financial damage (σ_j/δ_i).
$x(0), y(0)$	Initial financial resources of the exchange and the attacker at time $t = 0$, respectively.
g_1, g_2	Growth rates of financial resources for the exchange and the attacker.
$u(0), v(0)$	Total investment ratio chosen by the exchange and attacker ($0 \le u(0) \le 1, 0 \le v(0) \le 1$).
α_i, β_i	The proportion of the total investment allocated to specific strategies by the exchange and the attacker ($\sum\alpha_i = 1, \sum\beta_i = 1$).
r_1	Defense efficiency coefficient (protection ratio), empirically derived from prevented damage and countermeasure costs.
r_2	Attack effectiveness coefficient, derived from average potential damage and operational attack costs.
v^*	The calculated value of the infinite antagonistic game, representing the risk degree of achieving a goal.
μ^*, η^*	Optimal mixed strategies (probability measures) for the exchange and the attacker.
γ_k	Coefficients that determine the sets of players' preferences

V. RESULT AND DISCUSSION

The simulation environment was developed in Python using the PyCharm Professional Integrated Development Environment (IDE) within the Anaconda distribution. Computations were performed on a hardware platform with an Intel Core i7 processor and 32 GB of RAM. The main computational modules used NumPy and SciPy for matrix operations and to find Nash equilibria in mixed strategies. Instead of using a static, retrospective dataset, which quickly becomes outdated due to the rapid evolution of cyber threats in the cryptocurrency space, we employed a synthetic dataset generator. This generator utilized Monte Carlo methods to simulate the phase space of resources (x, y) and their corresponding growth factors (g_1, g_2). The resulting data was calibrated based on baseline periods of historical volatility for major centralized cryptocurrency exchanges to ensure realistic boundaries for the identified safe and critical risk zones.

Computational experiments were conducted in a simulated environment using synthetic datasets simulating various cryptocurrency market conditions. The priority metrics used for system evaluation were the probability of successful defense, determined by the values of optimal mixed strategies, the expected value of each side's win, determined by the game value v^*, and the system's resilience thresholds $x(1) \ge 0$.

A comparative analysis with static cybersecurity models [41, 42] showed that the proposed game-theoretic approach can account for the nonlinear nature of damage. While classical detection systems rely on static blocking thresholds, the proposed algorithm demonstrates that under Strategy 3, i.e., synchronization with market volatility, static defense budgets lose effectiveness.

Furthermore, with regard to Strategy 6 [24, 25] (i.e., the introduction of a third party), it was found that the inclusion of cyber insurance transforms the "Safe Zone." The insurer converts the exchange's stochastic risks into deterministic operating costs. The latter will allow the exchange to accept scenarios with $x(1) < 0$ (a temporary security breach) as an acceptable risk, provided this breach is fully covered by external insurance payments.

Let's consider several specific cases, see Figs. 2 and 3.

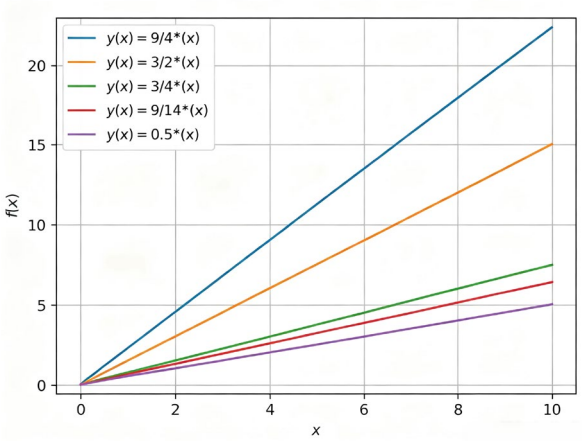

Fig. 2. Attacker and defender resource changes for Scenario $r_1 \times r_2 > 1$.

Fig. 2 demonstrates an unstable system state in which the product of the escalation factors exceeds unity, leading to exponential growth in costs for both parties. The solid lines represent the theoretical resource depletion boundaries calculated using Eq. (2), and the markers show the validation results based on simulation test data.

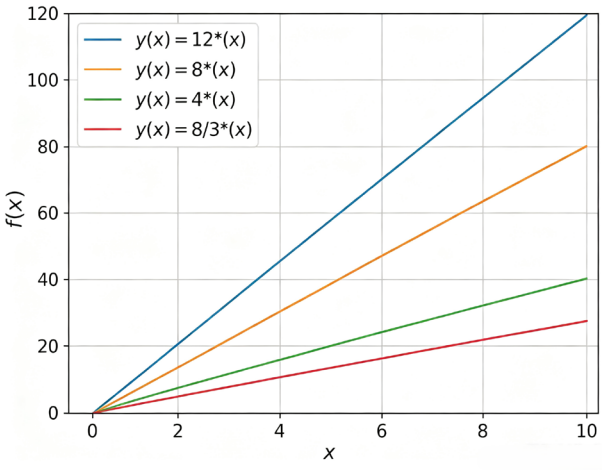

Fig. 3. Phase space of system states for the scenario $r_1 \times r_2 \le 1$.

The case $r_1 \times r_2 > 1$. In this case, we obtain that one of the coefficients r_1 or r_2 is strictly greater than the reciprocal of the coefficient of the other player. Therefore, Fig. 2 shows the sets of constancy of the game value in the area (2). In each set of game value constancy, the players have optimal mixed strategies. For example, if we have the following test case: $x^*(0) = 7, y^*(0) = 4, g_1 = 3, g_2 = 4, r_1 = 2, r_2 = 1$, then with such a set of input data the players have optimal mixed strategies μ^*, η^*. Measure μ^* is concentrated at points: $u_1^* = \frac{5}{21}, u_2^* = \frac{5}{7}$. Measure η^* is concentrated at points: $v_1^* = 1, v_2^* = \frac{3}{8}$. Measures μ^*, η^*. at these points have a value equal to $\frac{1}{2}$. The value of the game v^*, when players use optimal strategies, is $\frac{1}{2}$.

In addition, the following graph is obtained in PyChar, shown in Fig. 3. On a plane $(x(0), y(0))$, on which areas are indicated in which the game value takes different values.

In the second case $r_1 r_2 \leq 1$ the following set of input data is considered: $x^*(0) = 1,\ y^*(0) = 13, g_1 = 2, g_2 = \frac{1}{4}, r_1 = \frac{1}{2}, r_2 = 1$. In this case, the players have optimal pure strategies. For the first player, the optimal pure strategy will be $u_1^* = 1$, for the second player – $v_1^* = \frac{9}{13}$. Such a graph for this case is obtained in Fig. 3. on a plane $(x(0), y(0))$, on which areas are indicated in which the game value takes different values.

In the framework of the article, we focused only on these cases, because they show the most common situations in the interaction of the parties. We note the following circumstance. The result of the interaction of the players depends on many parameters, and if it does not satisfy the players, then they can change them (at least those that they can change) in order to obtain an acceptable result for them.

Fig. 2 shows the situation when the first player does not have the opportunity to find his optimal pure strategy, which will allow him to achieve his goal with probability 1. However, he has an optimal mixed strategy that will allow him to achieve it with probability $\frac{1}{2}$.

To test the model's practical validity, a series of additional computational experiments was conducted. The goal of this series was to compare the resulting mathematical solutions with the attack scenarios formulated in the introduction—Strategies 1–5. Unlike the initial analysis presented in Figs. 2 and 3, which only considered the players' winning or losing outcomes, we identified specific zones in the phase space of states corr (x, y) responding to different types of threats. During the experiment, resource parameters (x, y) and growth factors (g_1, g_2) were varied, simulating market volatility. This allowed transforming the linear graphs into a scenario zone map (see Figs. 4 and 5).

Fig. 3 shows the situation in which the second player, applying his optimal pure strategy, achieves his goal. The main factor that contributed to this was his advantage in the number of financial resources.

Table I below describes qualitative descriptions of strategies using a set of variable model parameters, such as the parties' initial resources (x_0, y_0) ,their growth rates (g_1, g_2) and investment efficiency ratios (r_1, r_2). The correspondence between attack scenarios and modeling parameter ranges is shown in Table II.

TABLE II. EXPERIMENTAL SETUP: MAPPING ATTACK SCENARIOS TO MODEL PARAMETERS

Strategy	Configuration of model parameters	Physical interpretation of parameters
$S1$	$y(0), x(0)$ $r_2 > 1/r_1$	Attacker has low initial resources (cheap spam), but high efficiency coefficient r_2 due to the law of large numbers.
$S2$	$y(0) \to x(0)$ High $y(0)$ cost	High entry threshold for the attacker (expensive preparation). The attack is comparable in cost to the defender's budget.
$S3$	g_1, g_2 Variable $g(t)$	Rapid growth of resource value due to market "pump". Reduces the relative effectiveness of static defense budgets.
$S4$	$r_1 \times r_2 \approx 1$ Mixed Strategies Area	Neither side has a decisive advantage. Continuous investment in r (efficiency) is required to shift the equilibrium.
$S5$	$x(t) < 0$ allowed Compensated externally	The defender accepts a negative outcome in the game (breach) but covers it via external insurance mechanisms (Strategy 6).

Note: An analysis of the effectiveness zones revealed the following results.

The effectiveness zone of mass phishing. Figs. 4 and 5, this zone corresponds to the low-value region $(y(0), x(0))$. Here, the attacker has significantly fewer resources than the exchange. This, accordingly, means a low cost of attack, i.e., Strategy 1. However, due to the high values of the attack efficiency coefficient, achieved through the mass distribution and the law r_2 of large numbers, it is capable of transferring the game to a state of mixed strategies or even winning. The experiment showed that without active defense adaptation $(r_1 \approx 0)$, this zone will expand. This makes CEX potentially vulnerable to even cheap attacks.

The dotted lines in Fig. 4 represent the mathematical boundaries, according to Eq. (1), that exclude overlapping regions. A one-to-one correspondence is shown: strategies S1 and S2 are applicable in the Safety Zone; strategies S3, S4, and S5 ("Arms Race") lie in the Parity Zone; strategy S6 (involvement of a third party) is activated only upon entering the Critical Risk Zone. The legend displays the parameters of the test data sets confirming the validity of the zoning.

Fig. 4 shows the simulation results, illustrating the relationship between the mathematically justified piecewise intervals of the payoff function and the three risk zones. Each zone has boundaries that exclude logical or mathematical overlap. This fully complies with the conditions laid down in the revised Eq. (1).

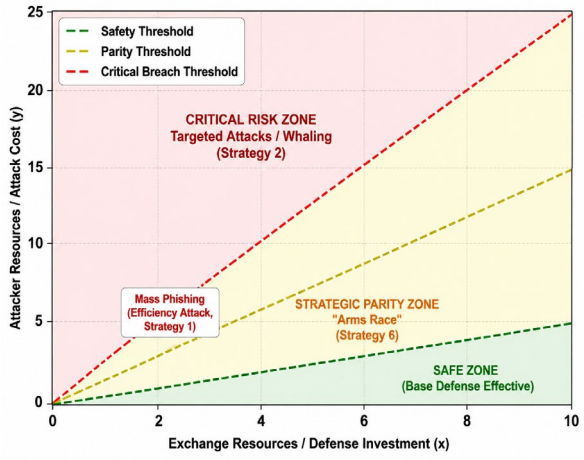

Fig. 4. Distribution of defense strategies (S1–S6) across three key risk zones: the security zone, the strategic parity zone, and the critical risk zone.

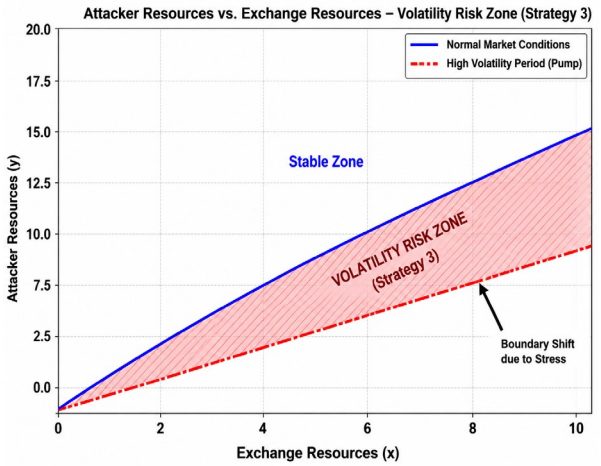

Fig. 5. Changing the exchange's security boundaries in conditions of high market volatility (implementation of strategy 3).

The graphical space is divided into the following regions, each of which is assigned its own set of optimal strategies (S1–S6):

(1) The Safe Zone is located in the lower left portion of the graph. In this area the threat level is controllable. This allows the defender to employ passive response strategies, such as Strategy 1 (Risk Acceptance) and Strategy 2 (Basic Risk Mitigation).

(2) The Strategic Parity Zone occupies the central part of the phase space. Here, the development of the conflict requires active resource allocation. This zone encompasses the application of Strategy 3 and Strategy 4 (Adaptive Response), and reaches its limit in the Arms Race scenario, which strictly corresponds to Strategy 5 (S5).

(3) The Critical Risk Zone is located beyond the upper boundary curve. Entering this region means the defender's internal resources are insufficient to counter the threat. The only mathematically sound solution here is to switch to Strategy 6 (S6) - transferring the risk to a third party, such as using cyber insurance.

The straight lines dividing the specified zones are constructed on the basis of empirical data sets (see Section V) and confirm the theoretical conclusions - the transition between strategies S1-S6 occurs exactly at the intersection points of the boundary conditions.

Computational experiments were carried out using the Anaconda distribution kit (PyChar Professional programming environment), which made it possible to visualize the results of the game and will be useful for analysts involved in the information security of trading platforms, specializing in the purchase and sale of DCC, and counteracting such a type of threat as phishing attacks.

The research's novelty lies in its proposed mapping of qualitative phishing attack scenarios on cryptocurrency exchanges—such as mass phishing, targeted attacks, exploitation of market volatility, and others—to the solution space of an infinite zero-sum game of resources. Unlike existing models, the developed model will allow determining the transition boundaries between defense strategies depending on the current volatility of the cryptocurrency market (g-parameters) and the attacker's technological sophistication (r-parameters). It has been proven that the exchange's "Safe Zone" is not constant. It deforms nonlinearly as market trends change, requiring the implementation of flexible mechanisms for managing the CEX information security budget.

Despite the obtained results confirming the effectiveness of the game-theoretic approach for modeling phishing attack scenarios, the proposed model has several limitations that open up avenues for further research. For example, in the current formulation, the game is considered a zero-sum game. That is, the attacker's gain is equivalent to the exchange's loss. However, when implementing Strategy 4, the exchange's damages can significantly exceed the attacker's direct profit. Furthermore, the introduction of insurance (Strategy 6) transforms the interaction into a non-zero-sum game. This requires a more complex mathematical model. In this experiment, the coefficients r_1 and r_2 are assumed to be constant for each individual iteration. In the "Arms Race" scenario (Strategy 5), these parameters will continuously change. Also, in its current form, the model assumes that both the exchange and the attacker act strictly rationally, striving for equilibrium. However, phishing attacks often exploit irrational user behavior, such as panic and greed. This introduces stochastic noise, which is not fully accounted for in current equations.

To demonstrate the direct relationship between the piecewise value intervals (v^*), defined in Eq. (1) and the three identified risk zones, we mapped the mathematical thresholds directly to the phase space scenarios.

Safe Zone (Basic Defense Effective). This zone is mathematically correlated with the game values at which the exchange deterministically neutralizes the threat ($v^* = 0$ or $v^* \to 1$). According to Eq. (1), this occurs when the exchange's resources significantly exceed the attacker's capabilities: $r_1 \times g_1 \times x(0) \geq g_2 \times y(0)$. In this interval, the exchange can rely on optimal pure strategies to maintain security without critical losses.

The zone of strategic parity ("Arms Race")—when the balance of resources and efficiency falls within intermediate piecewise intervals, the value of the game becomes fractional ($v^* \in (0,1)$ or $v^* \in (-1,0)$, for example, $v^* = \pm 1/k$). In these intervals, interaction will require the use of optimal mixed strategies. Neither side has an absolute advantage, which mathematically reflects the continuous evolutionary "Arms Race" (Strategy 5). The specific fractional value of v^* directly and quantitatively determines the probabilistic degree of risk.

The critical risk zone, i.e., targeted attacks. This threshold is crossed when the game value reaches its lower limit ($v^* = -1$). According to the conditions of the piecewise function, this occurs when the attacker's capabilities completely overwhelm the budget allocated for defense: $r_2 \times g_2 \times y(0) > (1 + r_1 \times r_2) \times g_1 \times x(0)$. This is where deterministic defense strategies fail, making the exchange highly vulnerable to targeted phishing attacks (Strategy 2).

To confirm that these mathematical results are fully consistent with our experimental observations, we test the refined formulas using the previously presented test data sets: below, we examine the zones of strategic parity. Consider the first set of simulation data, where $x(0) = 7$, $y(0) = 4$, $g_1 = 3$, $g_2 = 4$, $r_1 = 2$, $r_2 = 1$. Substituting these values into our model confirms that the condition $r_1 \times r_2 > 1$ is satisfied. Evaluating the resource matrices yields $g_1 \times x(0) = 21$ and $g_2 \times y(0) = 16$. Applying the piecewise function logic from Eq. (1) to this interval yields a game value $v^* = 1/2$. Since v^* is a fractional number requiring mixed strategies (with probability measures μ^*, concentrated at the points $u_1^* = 5/21$ and $u_2^* = 5/7$), this strictly mathematically transfers the system to the Zone of Strategic Parity (the yellow area in Fig. 4). This calculation is in perfect agreement with the experimental finding that neither party achieves deterministic dominance under these particular market parameters.

Let's check the boundary transitions. In the second simulation scenario, initialized with the values $x(0) = 1$, $y(0) = 13$, $g_1 = 2$, $g_2 = 1/4$, $r_1 = 1/2$, $r_2 = 1$, we observe $r_1 \times r_2 = 1/2 \leq 1$. The extreme disproportion in initial resources ($y(0)$ is significantly greater than $x(0)$) destroys parity. Mathematically, players are forced out of the range of mixed strategies and resort to optimal pure strategies ($u_1^* = 1, v_1^* = 9/13$). This proves that extreme systemic imbalances successfully (from a mathematical point of view) move the game from the Strategic Parity Zone to the deterministic edges of the Critical Risk Zone, confirming the graphical boundary shifts revealed during high market volatility (Strategy 3).

Based on the identified limitations and scenario analysis, we identify the following priority development areas. First and foremost, this is the transition to stochastic differential games. To more accurately model Strategy 3 (The Impact of Volatility), we plan to take into account stochastic processes on the CEX. This will allow for random fluctuations in the cryptocurrency market. The introduction of a third player, the "Insurer" (as part of Strategy 6), will require a transition to cooperative games or Stackelberg games, where the exchange (leader) chooses the level of protection, and the insurer (follower) determines the premium.

Thus, the presented work creates a theoretical basis for the construction of customizable Decision Support Systems (DSS), but requires further calibration on real anonymized data from cybersecurity incidents on CEX.

In its current version, the model assumes the strict rationality of players. However, the game price v^* can be considered a baseline, adjusted in real-world crypto exchange practice to account for stochastic noise caused by cognitive overload and user panic. Future research is expected to focus, among other things, on analyzing the model's sensitivity based on real historical incidents. For example, analyzing the Ledger wallet database leak will allow us to simulate a sharp decline in customer trust and calculate the necessary increase in security investments to restore the disrupted strategic parity.

A comprehensive comparative analysis highlights the advantages of the proposed game-theoretic framework over existing paradigms. Compared to traditional machine learning-based phishing detection systems [37, 38, 40], which inherently rely on static blocking thresholds and historical feature extraction, our model flexibly adapts to variations in attacker strategies. Moreover, while previous game-theoretic models in cybersecurity [26, 28] have primarily considered static, single-stage interactions or assumed linear damage functions, the proposed model takes into account nonlinear reputational damage. The latter is specific to cryptocurrency exchanges (Strategy 4). The model also takes into account the critical impact of market stress (Strategy 3). This continuous, multi-stage evaluation demonstrated that static defense budgets, common in standard optimization models [41–44], are fundamentally inadequate during periods of high market volatility. Accordingly, this requires flexible resource reallocation, which is provided by the proposed mathematical core for the decision support system.

VI. Conclusion

The study resulted in the development and testing of a mathematical decision support model based on the theory of infinite zero-sum games. The key result of the study was the construction of a scenario zone map, which identified three critical states in the interaction between an attacker and a crypto exchange: a safety zone, a strategic parity zone (i.e., an "arms race"), and a critical risk zone. The key practical conclusion is that trading platform security boundaries are not static. Their nonlinear deformation during sharp market fluctuations, known as "pumps," has been mathematically confirmed. This means that static cybersecurity budgets are incapable of providing adequate protection during periods of stress on crypto exchanges. Using the proposed model will allow crypto exchange information security analysts to dynamically reallocate resources and adjust anti-phishing strategies in a synchronized manner. This means that information security analysts will have a tool that can mathematically justify adapting defenses to the attacker's

new technological capabilities and the current volatility of the cryptocurrency market.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Volodimir Malyukov and Valery Lakhno conceived the study and designed the methodology; Volodimir Malyukov also provided resources, supervised the project, and secured funding; Valery Lakhno performed the investigation, managed project administration, and contributed to resources; Bakhytzhan Akhmetov assisted with methodology and took part in writing–review and editing; Atkeldi Ogan developed the software and carried out the formal analysis; Inna Malyukova validated the results and curated the data; Zhuldyz Alimseitova performed validation, handled visualization, and participated in writing—review and editing; all authors have read and approved the final version of the manuscript.

REFERENCES

[1] P. Xia *et al*., "Characterizing cryptocurrency exchange scams," *Computers and Security*, vol. 98, 101993, 2020.

[2] T. Moore and N. Christin, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed., *Lecture Notes in Comput. Sci.*, vol. 7859. Berlin, Heidelberg: Springer, 2013, pp. 25–33.

[3] T. Tarasova *et al*., "Accounting and features of mathematical modeling of the system to forecast cryptocurrency exchange rate," *Accounting*, vol. 6, no. 3, pp. 357–364, 2020.

[4] N. A. Bakar and S. Rosbi, "Autoregressive Integrated Moving Average (ARIMA) model for forecasting cryptocurrency exchange rate in high volatility environment: A new insight of bitcoin transaction," *International Journal of Advanced Engineering Research and Science*, vol. 4, no. 11, pp. 130–137, 2017.

[5] X. Li and C. A. Wang, "The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin," *Decision Support Systems*, vol. 95, pp. 49–60, 2017.

[6] B. Krishnamachari, Q. Feng, and E. Grippo, "Dynamic Curves for Decentralized Autonomous Cryptocurrency Exchanges," arXiv preprint arXiv:2101.02778, 2021.

[7] S. A. Monsalve *et al*., "Convolution on neural networks for high-frequency trend prediction of cryptocurrency exchange rates using technical indicators," *Expert Systems with Applications*, vol. 149, 113250, 2020.

[8] Y. Wang *et al*., "Analysis of cryptocurrency exchange rates vs USA dollars using a new dagum model," *Alexandria Engineering Journal*, vol. 64, pp. 645–658, 2023.

[9] G. Milunovich and S. A. Lee, "Cryptocurrency exchanges: Predicting which markets will remain active," *Journal of Forecasting*, vol. 41, no. 5, pp. 945–955, Aug. 2022.

[10] K. Oosthoek and C. Doerr, "From hodl to heist: Analysis of cyber security threats to bitcoin exchanges," in *Proc. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC),* 2020, pp. 1–9.

[11] A. Alkhalifah *et al*., "An empirical analysis of blockchain cybersecurity incidents," in *Proc. 2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE),* 2019, pp. 1–8.

[12] A. Alkhalifah, A. Ng, A. S. M. Kayes, J. Chowdhury, M. Alazab, and P. A. Watters, "A taxonomy of blockchain threats and vulnerabilities," in *Blockchain for Cybersecurity and Privacy*, 1st ed. Boca Raton, FL: CRC Press, 2020, pp. 3–28

[13] U. W. Chohan, "The Problems of Cryptocurrency Thefts and Exchange Shutdowns," in *The Cryptocurrency Market*, A. Saeedi and A. Al-Fattal, Eds., ser. Palgrave Studies in Financial Services Technology, Cham: Palgrave Macmillan, 2025, pp. 69–86.

[14] J. A. Ramirez, E. Rodriguez, and C. I. Valdez, "Long-range correlations and asymmetry in the Bitcoin market," *Physica A: Statistical Mechanics and its Applications*, vol. 492, pp. 948–955, 2018.

[15] Y. Ding and W. Chen, "Probing the mystery of cryptocurrency exchange: The case study based on MT. GOX," in *Proc. 2022 International Conference on Service Science (ICSS)*, 2022, pp. 297–304.

[16] O. Boireau, "Securing the blockchain against hackers," *Network Security*, vol. 2018, no. 1, pp. 8–11, 2018.

[17] J. Hu, Q. Luo, and J. Zhang, "The fluctuations of bitcoin price during the hacks," *International Journal of Applied Research in Management and Economics*, vol. 3, no. 1, pp. 10–20, 2020.

[18] I. Astrakhantseva, R. Astrakhantsev, and A. Los, "Cryptocurrency fraud schemes analysis," in *Proc. SHS Web of Conferences,* 2021, vol. 106, 02001.

[19] A. A. Andryukhin, "Phishing attacks and preventions in blockchain based projects," in *Proc.* 2019 *International Conference on Engineering Technologies and Computer Science (EnT),* 2019, pp. 15–19.

[20] S. Aggarwal and N. Kumar, "Attacks on blockchain," *Advances in Computers,* vol. 121, pp. 399–410, 2021.

[21] K. Mrazek *et a*l., "Risks in blockchain—A survey about recent attacks with mitigation methods and solutions for overall," in *Proc. 2022 IEEE International Conference on Electro Information Technology*, 2022, pp. 5–10.

[22] I. Makarov and A. Schoar, "Cryptocurrencies and decentralized finance (DeFi)," *National Bureau of Economic Research*, vol.1, 30006, pp. 141–215, 2022.

[23] A. F. Loe and E. A. Quaglia, "You shall not join: A measurement study of cryptocurrency peer-to-peer bootstrapping techniques," in *Proc. 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2231–2247.

[24] S. A. Kamran, S. Sengupta, and A. Tavakkoli, "Semi-supervised conditional GAN for simultaneous generation and detection of phishing URLs: A game theoretic perspective," arXiv preprint arXiv:2108.01852, 2021.

[25] G. L. Huillier, R. Weber, and N. Figueroa, "Online phishing classification using adversarial data mining and signaling games," in *Proc. ACM SIGKDD Workshop on Cyber Security and Intelligence Informatics*, 2009, pp. 33–42.

[26] X. Chen, X. Liu, L. Zhang, and C. Tang, "Optimal defense strategy selection for spear-phishing attack based on a multistage signaling game," *IEEE Access*, vol. 7, pp. 19907–19921, 2019.

[27] N. Figueroa, G. L'Huillier, and R. Weber, "Adversarial classification using signaling games with an application to phishing detection," *Data Mining and Knowledge Discovery*, vol. 3, no. 1, pp. 92–133, 2017.

[28] M. Wang and L. Song, "Efficient defense strategy against spam and phishing email: An evolutionary game model," *Journal of Information Security and Applications*, vol. 61, 102947, 2021.

[29] R. Phillips and H. Wilder, "Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites," in *Proc. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC),* 2020, pp. 1–8.

[30] W. Chen *et al*., "Phishing scam detection on ethereum: Towards financial security for blockchain ecosystem," in *Proc. Twenty-Ninth International Joint Conference on Artificial Intelligence,* 2020, vol. 7, pp. 4456–4462.

[31] Z. Gu, D. Lin, and J. Wu, "On-chain analysis-based detection of abnormal transaction amount on cryptocurrency exchanges," *Physica A: Statistical Mechanics and its Applications*, vol. 604, 127799, 2022.

[32] Data Breach Investigations Report (DBIR). (2024). [Online]. Available: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

[33] Cost of a Data Breach Report 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[34] ENISA Threat Landscape 2024. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[35] Adversarial Misuse of Generative AI. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
[36] Disrupting malicious uses of AI: OpenAI. [Online]. Available: https://openai.com/uk-UA/index/disrupting-malicious-ai-uses/
[37] E. Kytidou, T. Tsikriki, G. Drosatos, and K. Rantos, "Machine learning techniques for phishing detection: A review of methods, challenges, and future directions," *Intelligent Decision Technologies*, vol. 19, no. 6, pp. 4356–4379, 2025.
[38] A. J. Ade and P. A. Tijare, "Advanced modeling of AI, machine learning, and deep learning approaches for phishing attack Detection on the web," in *Proc. 2025 International Conference on Circuits, Controls and Communications (CCUBE)*, 2025, pp. 1–7.
[39] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "Detection and prevention of spear phishing attacks: A comprehensive survey," *Computers and Security*, vol. 151, 104317, 2025.
[40] H. Jabbar and S. A. Janabi, "AI-driven phishing detection: enhancing cybersecurity with reinforcement learning," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, pp. 1–21, 2025.
[41] G. M. Medina, K. K. C. Villar, and T. H. Bhuiyan, "Integrating IT and OT for cybersecurity: A stochastic optimization approach via attack graphs," *IEEE Access,* vol. 13, pp. 140578–140599, 2025.
[42] J. Polónio, J. Moura, and R. N. Marinheiro, "Towards automatic detection and mitigation of high-risk cybersecurity vulnerabilities at networked systems," *IEEE Access*, vol. 13, pp. 181957–181976, 2025.
[43] B. Akhmetov *et al*., "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
[44] V. Lakhno *et al*., "Development of a model for decision support systems to control the process of investing in information technologies," *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 3, pp. 74–81, 2020.