

A neuro-game model for analyzing strategies in the dynamic interaction of participants of phishing attacks

Valery Lakhno^{1,5}, Volodimir Malyukov¹, Inna Malyukova², Bakhytzhan Akhmetov^{3,5}, Zhuldyz Alimseitova^{4,5}, Atkeldi Ogan^{4,5}

¹Department of Computer Systems, Networks, and Cybersecurity, Faculty of Information Technology, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine

²Rating agency "Expert-rating", Kyiv, Ukraine

³Department of Informatics and Informatization of Education, Physics and Computer Science, Institute of Mathematics, Kazakh National Pedagogical University named after Abai, Almaty, Kazakhstan

⁴Department of Cybersecurity, Information Processing, and Storage, Institute of Automation and Information Technology, Satbayev University, Almaty, Kazakhstan

⁵Department of Information Systems, Faculty of Engineering and Information Technology, Almaty Technological University, Almaty, Kazakhstan

Article Info

Article history:

Received Dec 23, 2023

Revised Feb 9, 2024

Accepted Feb 27, 2024

Keywords:

Artificial neural network

Cryptocurrency

Game model

Information security

Phishing

ABSTRACT

A dynamic model of countering phishing attacks is considered. Cryptocurrency exchanges (CCE) and/or their clients are considered as an example of a phishing victim. The model, unlike similar ones, is based on the assumption that the dynamics of the states of the player-victim of phishing attacks and the player-intruder (fisher) is set by means of a system of differential equations. The peculiarity of this model is that it represents a bilinear differential game of quality, for which methods for solving linear differential games are not applicable and, in addition, the absence of functional restrictions on the strategies of players (even immeasurable functions are allowed) does not allow the use of traditional approach. And their solution makes it possible to form payoff matrices, which are part of the training set for artificial neural networks (ANNs). Such a collaboration of models will make it possible to accurately build an anti-phishing strategy, minimizing the costs of both a potential victim of phishing attacks and the defense side when building a secure system of communication with CCE clients. The neuro-game approach makes it possible to predict the process of countering phishing in the context of costs for both parties using different strategies.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Zhuldyz Alimseitova

Department of Cybersecurity, Information Processing, and Storage

Institute of Automation and Information Technology, Satbayev University

050000 Almaty, Kazakhstan

Email: zhuldyz_al@mail.ru

1. INTRODUCTION

A phishing attack is perhaps one of the simplest and least expensive ways for an attacker to obtain information about users. Since phishing attacks do not actually require high qualifications of hackers and are not associated with costs, they are very popular among both professional hackers and various kinds of computer scammers. The popularity of this method of obtaining information about the user gives rise to a large number of tactics for conducting a phishing attack. We can say that at the simplest level, attackers resort to a simple mailing of letters containing, for example, a link to a malicious site or an attached file.

With a more sophisticated tactic, this can be phishing, supplemented with elements of social engineering. For example, in 2019, a similar phishing attack was recorded in Venezuela [1]. A website was created where volunteers registered to participate in the humanitarian action. For registration, it was necessary to indicate personal data, an identity document, and a mobile phone number. The attacker managed to actually create an identical site. With a very similar domain. As a result, the personal information of thousands of volunteers was actually stolen [2].

Phishing is a serious threat to ordinary users. For example, as the popularity of cryptocurrencies (CC) and accordingly various cryptocurrency exchanges (CCE) grows, many users began to actively explore this area, hoping to make quick money. And since often many users, who do not have elementary knowledge in the field of information security (IS), try to make a quick profit, such owners of crypto wallets are in the first row of potential victims of phishing attacks, since they most likely will not notice or ignore the tricks that attackers use to steal personal data. So, in 2019, there were many reports in the press about the use of phishing to steal funds from one of the crypto wallets on the binance CCE [3]. The CCE said that the attackers stole 7,000 bitcoins. This for 2019 is approximately 2% of all binance bitcoin assets. To steal these funds, hackers used phishing and virus attacks to obtain sensitive user data from many customers, including two-factor authentication codes. As noted in [3] "Hackers had the patience to wait for a favorable moment and carry out a well-planned operation through many accounts that at first glance seemed completely independent." The ever-present threat of phishing attacks motivates IS researchers to look for new techniques and technologies to counter phishing. In particular, such technologies can be based on the use of artificial neural networks (ANNs), which can filter out phishing emails or identify phishing sites with a high degree of efficiency.

The authors of [2], [4] considered traditional methods of countering phishing attacks. For example, according to the authors, the uniqueness of the site design, the use of one-time passwords, and one-way authentication can become an effective method of counteraction. It is difficult to argue with this, however, we note that each of these methods leads to an increase in the cost of developing and/or maintaining the site for the owner. Even such a policy does not always lead to success. So, for example, in 2021, a fake website of one of the largest banks in Ukraine was revealed [5]. Fraudsters lured clients into non-existent projects, offering high income under a scheme that has the properties of a financial pyramid using social engineering methods and likely hacking.

A similar scheme with a fake website of a CCE is described in [6]. The authors of the publication cite as an example the situation when one of the most famous fake CCE was exposed in South Korea in 2017. The fake CCE was called BitKRX, so that customers would associate the name with the largest South Korean financial trading platform-Korea exchange (KRX). As a result, customers who thought they had bought bitcoin (BTC) and tried to access their funds found that their money had simply disappeared [7]. Spear phishing on CCE is a type of cyber attack in which attackers send hyperlinks, for example, using email, to well-researched targets [8], [9]. The purpose of such attacks is to obtain sensitive information by imitating trusted websites.

The researchers [10], [11] consider both classical and new methods of protection against phishing attacks. For example, according to the researchers, in some cases, it is enough to simply increase the level of information culture of clients of financial institutions in order to avoid the consequences of phishing. The most advanced technological solutions involve the introduction of gateway solutions to combat phishing attacks or machine learning technologies, such as ANN, to recognize phishing sites.

It is shown that it is possible to detect phishing websites using ANN [12]-[17]. Of course, this is not a complete list of scientific papers devoted to the study of the effectiveness and expediency of using the ANN apparatus to combat phishing sites and phishing emails. In particular, these papers show that ANNs can be used to detect and prevent phishing attacks due to their strong active learning ability on massive datasets and high data classification accuracy. However, repeated points in public datasets, as well as some features in feature vectors, complicate ANN training. Also, we noticed that most of the authors who offer certain ANNs practically do not touch upon the cost of creating such a network for its training and retraining when the attacker changes phishing tactics.

Meanwhile, the attacker's relationship i.e. fisher and his potential victim can be described as the interaction of players [18]. In this research, the authors introduce an approach according to which the game between IDS agents and insiders was adapted. The solution of the phisher's intention forecasting following the previous actions of both players was based on the usage of quantal response equilibrium (QRE) in game theory. The game was modeled to cover as many enemy strategies as possible. However, the authors focus on a variety of phisher's strategies, ignoring the relationship between players' strategies and the financial costs of achieving their goals.

An attacker (phisher) using the techniques of phishing attacks (often targeted) tries to penetrate cyber systems, for example, CCE to obtain confidential information. This can be done, for example, through

interaction with CCE staff or its clients. That is, there are two sides-the attacker and the victim. The game theory apparatus can be used in different ways. The researchers [18], [19] propose approaches according to which game theory makes it possible to gain knowledge about the interaction between the fisher and the victim in order to predict the next actions of the fisher in accordance with information from past interactions and recommend actions on the side of the victim. These works describe the game in such a way that it is possible to predict the future intentions of the fisher in accordance with the past actions of both players. For example, the authors consider such iterations of the strategies of the parties:

- a. phisher: use of a fake attachment (or link); victim: use an antivirus;
- b. phisher: masking the content of e-mail; victim: anti-phishing training.

Of course, this is not a complete list of possible strategies of the parties. Well, from such a simple set, in terms of cost, additional questions arise. For example, which antivirus is preferable for the victim side? Is it enough to limit yourself to the basic set of protective functions of an antivirus, for example, provided by many free antiviruses, or is it preferable to invest in more advanced paid versions that also provide protection against phishing? Or how to organize customer training? Let's say the CCE issues a detailed instruction or organizes an online training, involving information security practitioners (and they are likely to require payment for their services).

Similarly, other pairs of action strategies of the fisher side and the victim or defense can be constructed. Thus, the researchers in [20], [21] show that in order to protect against phishing attacks, you can use both built-in tools in browsers and mail servers, as well as overlay tools provided by third-party vendors. How effective are such solutions compared to user training and whether it is necessary to buy an additional system to combat phishing, the authors do not consider.

The researchers [17], [22] using game theory, focus on the calculation of the Nash equilibrium in mixed strategies for the attacker-defender game and present a rational scheme for obtaining an advantage that the attacker has over the defender. The reviewed papers propose a zero-sum non-cooperative spear-phishing model. This allows an attacker (such as a phisher) to choose the optimal strategy in order to maximize the payoff. However, the authors did not at all touch upon this aspect of the problem of choice, the choice of one or another variant of the defense and attack strategy in the context of its influence on the costs of the parties to the game.

Actually, all of the above and predetermined our interest in this topic. As is known, the synthesis of various methods and models, the use of tools from different fields of science, often leads to good results. This, for example, refers to the collaboration between the game theory apparatus and neural networks. Such a combination can be very interesting when solving problems related to predicting the outcome of the confrontation between the parties, when assessing the impact of their costs on protection and overcoming it, in particular, for the case of a phishing attack on the CCE.

Conceptually, the interaction of these two fundamental sections of mathematics is based on the assumption that individual neurons, for example, in an ANN, will behave optimally when activated in accordance with a given payoff matrix. Such a payoff matrix can be generated, for example, by solving a conventional matrix game or by solving a bilinear differential or multi-stage quality game with several terminal surfaces. Thus, it is natural to assume that game theory can act as a basic organizing principle for the formation of such an ANN. In other words, game theory makes it possible to generate, in our case, a payoff matrix by solving a bilinear differential quality game with several terminal surfaces [23]. This means that game theory acts as a guiding principle in the organization and communication of neurons in an ANN used to combat phishing, in the context of the cost of different strategies for the victim and/or the defense side, for example, the information security administrator of the CCE.

Also, the rational (optimal) strategy of the player (victim or defender) can be used when choosing the optimal learning parameters (convolution) of the ANN. The game model presented in this article for protecting CCE from phishing attacks can be considered as a stage in the construction of an ANN. The experience of successful implementation of ANN in the tasks of countering phishing gives us reason to assert with confidence that ANN, due to its advantages in comparison with other approaches, will effectively identify hidden statistical and other dependencies of phishing attacks, as well as obtain non-obvious and non-trivial results. In our opinion, such a combination of two fundamental theories-games and neural networks, makes it possible to effectively solve the problem of combating phishing through the development of intelligent information systems to support decision-making in various applied tasks, combating CCE phishing. Purpose and objectives of the study: development of a neuro-game approach for the analysis of optimal strategies in the dynamic interaction of participants in phishing attacks and the choice of an option that minimizes the cost of protection. To achieve the goal of the study, it is necessary to solve the following tasks: based on the model for solving a quality differential game with several terminal surfaces, to develop an approach that allows to generate payoff matrices that are part of a training set for ANNs; to carry out testing of the model and initial training of the simplest ANN.

2. METHOD

In order to obtain an effective result in the fight against phishing, a synthesis of two approaches is used-gaming and neural networks. The game approach serves, in this case, as the basis for forming part of the training set for the ANN. Alexa, DMOZ data for genuine sites and PhishTank, OpenPhish for phishing sites can be used as the main part of the training set [24]. In this paper, we mainly consider a game model that describes the interaction between a fisher and his potential victim. Such a game model is a bilinear differential quality game with several terminal surfaces. We present the setting of the game model.

2.1. Problem statement

The situation when, during the trading sessions on the CCE, a fisher tries to inflict damage (primarily financial) to the participants is, unfortunately, already standard. The natural response to this is to create tools to counter it. The model proposed below is an attempt to increase the arsenal of such anti-phishing tools. Moreover, the costs on the part of the victim in (and/or protection) certain technical means and methods of countering phishing are analyzed. The model describes the interaction between a bidder (a potential victim) and a fisher, which is a time-continuous procedure. The attacker tries to cause damage through phishing attacks. In future, we will call them the first and second players, respectively.

The interaction takes place in the following way. The first player has technological strategies to counter the attacks of the second player. This, for example, is partial ignoring of false information, its avoidance, ignoring letters, and SMS. To harm the first player, the second player has technological strategies, such as social engineering, the use of keyloggers, and email password stealers. The use by the second player of his technological strategies leads to financial losses.

Note that, for example, the built-in information security tools of mail services and browsers provide only a basic level of protection against phishing. Skilled attackers are able to bypass such tools because they have the ability to test the relevant mechanisms before the attacks are launched. Overlay means, implement more complex algorithms. Although these algorithms can also be studied by cybercriminals, however, this significantly increases the cost of attacks. That is, it will increase the need for the second player to have the appropriate financial resources (FR). Indeed, the phisher will have to purchase appropriate verification and testing solutions. Not all phishers are ready to take such a step.

Accordingly, more expensive means form a "safety window" that provides effective protection. Let us denote by δ_i – the amount of financial damage that the second player inflicts on the first player by applying his i -th technological strategy; by σ_j – the amount of financial income that the first player will receive when he applies his j -th technological strategy; by s_{ij}^1 –ratio of δ_i/σ_j , by s_{ij}^2 – ratio of σ_j/δ_i . If $\delta_i = 0$ at some i or $\sigma_j = 0$ at some j , then we exclude them from consideration. At the point in time t ($t \in [0, \infty)$) the first player in the framework of operations on the CCE, having a financial resource (hereinafter FR) $h_1(t)$, converts it to $g_1 \cdot h_1(t)$ (g_1 - growth rate of his FR). Then, by choosing his strategy $u(t): 0 \leq u(t) \leq 1$, he determines the amount of his investments in the technological aspects of ensuring the information security of trading sessions on the CCE - $u(t) \cdot g_1 \cdot h_1(t)$. It is believed that the structure of investment by him of his technological strategies is given. This structure is given by the set: $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_M: 0 \leq \alpha_i \leq 1, \sum_{i=1}^M \alpha_i = 1$ (M – number of technological strategies of the first player), i.e. the amount of investment can be written as: $u(t) \cdot g_1 \cdot h_1(t) = \alpha_1 \cdot u(t) \cdot g_1 \cdot h_1(t) + \dots + \alpha_M \cdot u(t) \cdot g_1 \cdot h_1(t)$.

The value $\alpha_j \cdot u(t) \cdot g_1 \cdot h_1(t), j = 1, \dots, M$ compensates for $\sum_{i=1}^N s_{ij}^1 \cdot \alpha_j \cdot u(t) \cdot g_1 \cdot h_1(t)$ losses from the actions of the second player. This determines the decrease in the value of his FR by this value. Therefore, the total compensation for the losses of the fisher (the second player) from the investment of the first player in anti-phishing defenses is equal to: $\sum_{j=1}^M \sum_{i=1}^N s_{ij}^1 \cdot \alpha_j \cdot u(t) \cdot g_1 \cdot h_1(t)$. Let us denote by r_1 the coefficient $\sum_{j=1}^M \sum_{i=1}^N s_{ij}^1 \cdot \alpha_j$. At the point in time t ($t \in [0, \infty)$) fisher (second player) has $h_2(t)$ FR, which he intends to spend on organizing phishing attacks. The second player, having at the moment of time t ($t \in [0, \infty)$), $h_2(t)$ of FR, converts them to $g_2 \cdot h_2(t)$ resources (here g_2 – first player's FR growth rate). Then, by choosing his strategy $v(t): 0 \leq v(t) \leq 1$, he determines the value $v(t) \cdot g_2 \cdot h_2(t)$. We believe that the structure of investment by him of his technological strategies is given, which is given by the set: $\beta_1, \beta_2, \beta_3, \beta_4, \dots, \beta_N: 0 \leq \beta_i \leq 1, \sum_{i=1}^N \beta_i = 1$ (N –the number of technological strategies of fisher (the second player)). Or it can be written as follows: $v(t) \cdot g_2 \cdot h_2(t) = \beta_1 \cdot v(t) \cdot g_2 \cdot h_2(t) + \dots + \beta_N \cdot v(t) \cdot g_2 \cdot h_2(t)$.

The value $\beta_i \cdot v(t) \cdot g_2 \cdot h_2(t), i = 1, \dots, N$ levels $\sum_{j=1}^M s_{ij}^2 \cdot \beta_i \cdot v(t) \cdot g_2 \cdot h_2(t)$ income from the actions of the first player. For example, if he chose the right anti-phishing strategy and, accordingly, invested in successful technological solutions that effectively implement anti-phishing protection. This determines that the FR of the first player will decrease by this amount. That is, the total leveling of the FR of the first player from the investments of the second player is equal to: $\sum_{j=1}^N \sum_{i=1}^M s_{ij}^2 \cdot \beta_i \cdot v(t) \cdot g_2 \cdot h_2(t)$. Let us denote by

r_2 the coefficient $\sum_{j=1}^N \sum_{i=1}^M s_{ij}^2 \cdot \beta_i$. Then the FR of the players at the moment of time t ($t \in [0, \infty)$) will satisfy the following system of differential (1) and (2):

$$dh_1(t)/dt = -h_1(t) + g_1 \cdot h_1(t) - u(t) \cdot g_1 \cdot h_1(t) - r_2 \cdot v(t) \cdot g_2 \cdot h_2(t); \quad (1)$$

$$dh_2(t)/dt = -h_2(t) + g_2 \cdot h_2(t) - v(t) \cdot g_2 \cdot h_2(t) - r_1 \cdot u(t) \cdot g_1 \cdot h_1(t); \quad (2)$$

The conditions for the end of the interaction of players at the moment of time t ($t \in [0, \infty)$) will be the fulfillment of conditions (3) or (4):

$$h_1(t) > 0, h_2(t) = 0; \quad (3)$$

$$h_1(t) = 0, h_2(t) > 0; \quad (4)$$

$$h_1(t) = 0, h_2(t) = 0; \quad (5)$$

If it turns out that condition (3) is satisfied, then we will say that in the interaction of players at the moment of time t ($t \in [0, \infty)$) the first player has achieved the desired result and the interaction procedure is over. For the first player, his expenses (investments) for carrying out measures to protect against phishing attacks turned out to be successful, and the chosen strategies will bring him a win. If it turns out that condition (4) is satisfied, then we will say that in the interaction of players at the moment of time t ($t \in [0, \infty)$) the second player has achieved the desired result and the interaction procedure is over. For the second player, his expenses (investments) for conducting a phishing attack turned out to be successful, and the chosen strategies will bring him a gain.

If it turns out that condition (5) is satisfied, then we will say that in the interaction of players at the moment of time t ($t \in [0, \infty)$) both players did not achieve the desired result and the interaction procedure is over. If neither condition (3), nor condition (4), nor condition (5) are satisfied, then the procedure for the interaction of players continues further for time points $\tau: \tau > t$. Let us denote by $T^* = [0, \infty)$ the time variable change set.

The first player, based on the available information, can determine the amount of FR that he needs to allocate to counter the second player (fisher). The amount of FR spent also affects how effective anti-phishing protection will be. Indeed, the cost of creating an effective filter to block phishing sites and phishing emails will cost CCE many times more than just explaining to customers the danger of opening suspicious emails. The second player chooses his strategy $v(\cdot)$ based on any information. The first player seeks to find the set of initial FFs and initial states $h_2(0)$ of the first and second players, which have the following property, described by us in the paper [25]. *Property*: if the game starts from them, then the first player can, by choosing his strategy $u_*(\cdot, \cdot, \cdot)$, to ensure at one of the points of time t the fulfillment of the condition (3). At the same time, this strategy, chosen by the first player, contributes to preventing the fisher (second player) from fulfilling conditions (4), (5) at previous moments of time.

The set of such states is the preference set of the first player W_1 . Accordingly, the strategies $u_*(\cdot, \cdot, \cdot)$ of the first player with the indicated properties are his optimal strategies. The goal of the first player is to find the preference set and optimal strategies, applying which he will obtain the fulfillment of condition (3). According to the classification of decision theory, the formulated game model corresponds to the problem of decision making with complete information. Moreover, such a model is a bilinear quality differential game with several terminal surfaces. Finding the preference sets of the first player and his optimal strategies depends on a set of parameters.

In order to form the corresponding part of the training set for the ANN, we find the solution to the problem using the tools of the quality differential games theory [25]. This part of the training set is formed as a result of solving the problem from the point of view of the first player. That is, i.e. sets of "preferences" and optimal strategies $u_*(\cdot, \cdot, \cdot)$ are found for all ratios of game parameters. The solution of the problem from the point of view of the second player is similar.

2.2. Solution of the problem

The solution of the problem depends on the ratio of the interaction parameters. Various cases of parameter relations were considered in [25]. Therefore, we confine ourselves to a brief listing of them, presented in Table 1.

Table 1. Cases of the game parameters and dependencies ratio to determine the area of preference for player 1 and his optimal financial strategy to counter phishing attacks

Options	The set of "preferences" and the optimal strategy are found by the formulas:
1. $r_1 \cdot r_2 = 1, g_2 \geq g_1$	$W_1 = \{(h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, g_2 h_2(0) < r_1 \cdot g_1 \cdot h_1(0)\}$ $u_*(h_1(0), h_2(0)) = \begin{cases} 1, (h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ g_2 h_2(0) < r_1 \cdot g_1 \cdot h_1(0) \end{cases}$ and not defined otherwise.
2. $r_1 \cdot r_2 = 1, g_2 < g_1$	$W_1 = \{(h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ g_2 h_2(0) < r_1 \cdot g_1 \cdot h_1(0)\}$ $u_*(h_1(0), h_2(0)) = \begin{cases} 0, (h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ g_2 h_2(0) < r_1 \cdot g_1 \cdot h_1(0) < g_1 h_2(0) \end{cases}$ $u_*(h_1(0), h_2(0)) = \begin{cases} 1, (h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ g_2 h_2(0) < r_1 \cdot g_1 \cdot h_1(0) \end{cases}$ and not defined otherwise.
3. $r_1 r_2 > 1, g_2 > r_1 \cdot g_1 \cdot r_2$	Similar to option 1.
4. $r_1 r_2 > 1, g_1 \leq g_2 < r_1 \cdot g_1 \cdot r_2$	$W_1 = \{(h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ (r_1 g_1 r_2 g_2)^{0.5} h_2(0) < r_1 \cdot g_1 \cdot h_1(0)\}$ $u_*(h_1(0), h_2(0)) = \begin{cases} 1, (h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ (r_1 g_1 r_2 g_2)^{0.5} h_2(0) < r_1 \cdot g_1 \cdot h_1(0) \end{cases}$ and not defined otherwise.
5. $r_1 r_2 > 1, g_1 / (r_1 r_2) < g_2 < g_1$	Similar to option 4.
6. $r_1 r_2 > 1, g_2 < g_1 / (r_1 r_2)$	$W_1 = \{(h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, r_2 g_2 h_2(0) < g_1 \cdot h_1(0)\}$ $u_*(h_1(0), h_2(0)) = \begin{cases} 0, (h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ r_1 g_1 r_2 h_2(0) < r_1 g_1 h_1(0) < g_2 \cdot h_2(0) \end{cases}$ $u_*(h_1(0), h_2(0)) = \begin{cases} 1, (h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ r_1 g_1 h_1(0) > g_2 \cdot h_2(0) \end{cases}$ and not defined otherwise.
7. $r_1 r_2 < 1, g_2 \geq g_1$	Similar to option 1.
8. $r_1 r_2 < 1, r_1 g_1 r_2 \leq g_2 < g_1$	$W_1 = \{(h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ r_2 g_2 h_2(0) < g_1 \cdot h_1(0)\}$ $u_*(h_1(0), h_2(0)) = \begin{cases} 0, (h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ r_1 g_2 r_2 h_2(0) < r_1 g_1 h_1(0) < g_1 \cdot h_2(0) \end{cases}$ $u_*(h_1(0), h_2(0)) = \begin{cases} 1, (h_1(0), h_2(0)): (h_1, h_2) \in \text{int } R_+^2, \\ r_1 g_1 h_1(0) \geq g_1 \cdot h_2(0) \end{cases}$ and not defined otherwise.
9. $r_1 r_2 < 1, g_2 < r_1 \cdot g_1 \cdot r_2$	Similar to option 8.

In the same way, *problem 2* is solved from the point of view of the second player (fisher). Then, when forming a part of the training sample for the ANN, which will contain the results of the implementation of the set of game outcomes, it will be possible to represent a positive orthant in the plane $(h_1(0), h_2(0))$ in the form of three sets (cones with a vertex at a point $(0,0)$). One set (cone) adjacent to the axis $0H_1$, is the preferred set for the first player (the victim of a phishing attack). The second set (the cone) is the preferred set for the second player (the fisher). The third set (cone) is neutral from the point of view of both players. In fact, this set characterizes the balance property for players engaged in confrontation due to phishing attacks. Under certain ratios of the parameters of the opposition of the players, the balance set is a balance ray. That is, the players, for the states belonging to this set, have strategies that allow the players to continue the process of confrontation for a long time, as they like. This means that the conditions $(h_1(0), h_2(0)) \in R_+^2$ will be fulfilled for any point in time t .

Note that the rays, which are the boundaries of the cones, are specified by means of coefficients, which are a combination of parameters that specify the dynamics that describe the process of confrontation between the players. Therefore, if the initial values of the $(h_1(0), \phi(0))$ FR of the confrontation sides are given, then you can, for example, vary these parameters. In particular, to require that the parameters that determine the dynamics of the FR change are such that, the point $(h_1(0), h_2(0))$ is in the balance area, or, on the balance ray, if the cone separating two preference sets is the ray. If, however, some parameters are fixed

that determine the dynamics of FR changes, then it can be required that the values $(h_1(0), h_2(0))$ and part of the non-fixed parameters be such that the point $(h_1(0), h_2(0))$ falls into the area of balance. This, in turn, can affect both the confrontation process itself and recommendations when choosing strategies by players, primarily this applies to potential victims of phishing, as well as the defense side. If nothing can be changed, then the above solution of the game in problem 1, or the solution of the game in problem 2, will indicate the possible result of the confrontation procedure, under the assumptions under which problems 1 and 2 were considered.

Thus, the solution of the considered game, which made it possible to find the strategies of two players—a potential victim of phishing and a phisher, makes it possible to form a payoff matrix that is part of the training sample for the ANN. This payoff matrix horizontally has a finite set of groups of parameters of a potential phishing victim, and vertically there is a finite set of groups of phisher parameters. Each player can choose his own group of parameters. These groups of parameters (phishing victims) serve to describe a specific game (potential phishing situation). Since the game is solved for all ratios of game parameters, one of the values (+1, 0, -1) can be set at the intersection of the horizontal and vertical lines in the payoff matrix. Solving this matrix game and finding the value of the game in mixed strategies and optimal mixed strategies, we get that the situation with phishing on the CCE will be either positive (if the value of the game is positive), or negative (if the value of the game is negative), or neutral (if the value of the game is zero). This gives grounds for choosing the appropriate training set of player parameter groups into the payoff matrix. The obtained results of the game, as mentioned above, can be used to form part of the ANN training sample. At this stage, the purpose of training the ANN is to determine its weight coefficients.

3. RESULTS AND DISCUSSION

The model proposed in the work was implemented as a software module for analyzing the strategy of the defense side to counter phishing attacks for the CCY and/or their clients. The computational experiment was carried out using the Anaconda distribution kit (PyChar professional programming environment), on a PC with an i7 processor, and 32 GB of RAM. The computational experiment made it possible to visualize the results of the game between the victim of a phishing attack and an attacker (a phisher implementing different tactics of phishing attacks). The goal is to analyze the costs of the parties during the game and, accordingly, collect data for a part of the total array of ANN training sample, which is part of a larger project to use ANN to recognize phishing addresses and messages, for example, addressed to CCY clients. The result of the game implemented during the computational experiment is shown in Figure 1.

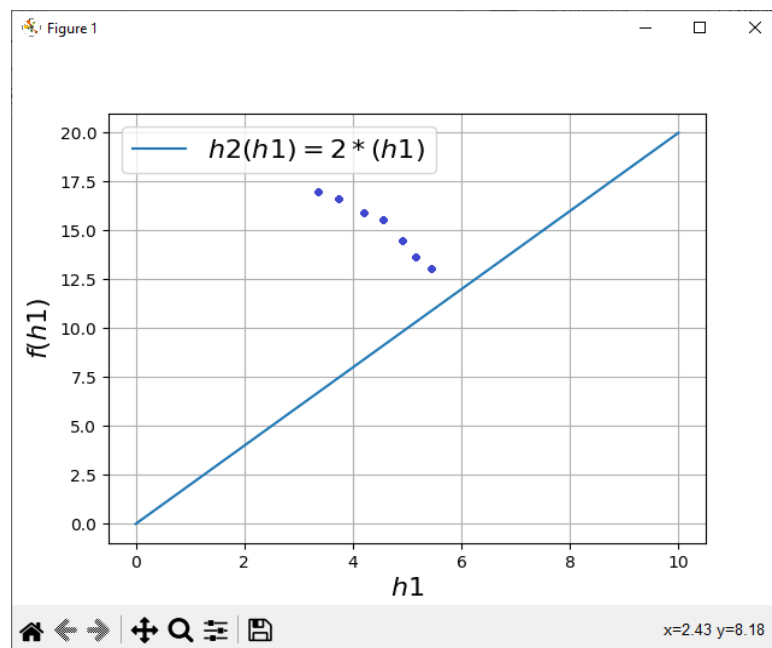


Figure 1. Results of the computational experiment. The trajectory of the movement of the second player (intruder)

Computational experiments, which are based on finding a solution to the bilinear differential quality game considered in the work, make it possible to form payoff matrices, which are necessary components for the functioning of the ANN. Note that a standard linear programming package can be used to solve matrix games by reducing a matrix game to a linear programming problem. Examples of the simplest matrix games generated by the bilinear differential quality game for ANN.

Example 1)

$$\begin{pmatrix} 100000 \\ 010000 \\ 001000 \\ 000100 \\ 000010 \\ 000001 \end{pmatrix},$$

the value of the game is $1/6$; Optimal mixed strategies-the choice of each pure strategy by the players with a probability of $1/6$. The phishing situation is positive.

Example 2)

$$\begin{pmatrix} -100000 \\ 0 - 10000 \\ 00 - 1000 \\ 000 - 100 \\ 0000 - 10 \\ 00000 - 1 \end{pmatrix},$$

the value of the game is $-1/6$; Optimal mixed strategies-the choice of each pure strategy by the players with a probability of $1/6$. The phishing situation is negative.

Example 3)

$$\begin{pmatrix} 1 - 1 \\ 0 + 1 \end{pmatrix},$$

the value of the game is $1/3$; Optimal mixed strategies-the choice of each pure strategy by the players with a probability $1/3$ and $2/3$. The phishing situation is positive.

Example 4)

$$\begin{pmatrix} -1 + 1 \\ 0 - 1 \end{pmatrix},$$

the value of the game is $-1/3$; optimal mixed strategies - the choice of each pure strategy by the players with a probability $1/3$ and $2/3$. The phishing situation is negative.

Example 5)

$$\begin{pmatrix} -1 + 1 \\ +1 - 1 \end{pmatrix},$$

the value of the game is 0 ; optimal mixed strategies-the choice of each pure strategy by the players with a probability $1/2$. The phishing situation is neutral.

Example 6)

$$\begin{pmatrix} +1 - 1 \\ -1 + 1 \end{pmatrix},$$

the value of the game is 0 ; optimal mixed strategies-the choice of each pure strategy by the players with a probability $1/2$. The phishing situation is neutral.

ANN training was carried out by analyzing the local outcomes of the games described above (respectively, options 1-9 presented in Table 1). A large number (about 250) of local games played and their results were automatically fed into the ANN in the form of a perceptron (the MATLAB environment was used-the neural network toolbox application package). As a result of training the ANN, the corresponding values of the coefficients of connections were obtained, and the dispersion of the learning results of the ANN was determined. The dispersion is presented on Figure 2. Thus, we can take the standard deviation of the accuracy of the model on the test set as an estimate of the dispersion of the predictions of the results of the game outcomes made using our model.

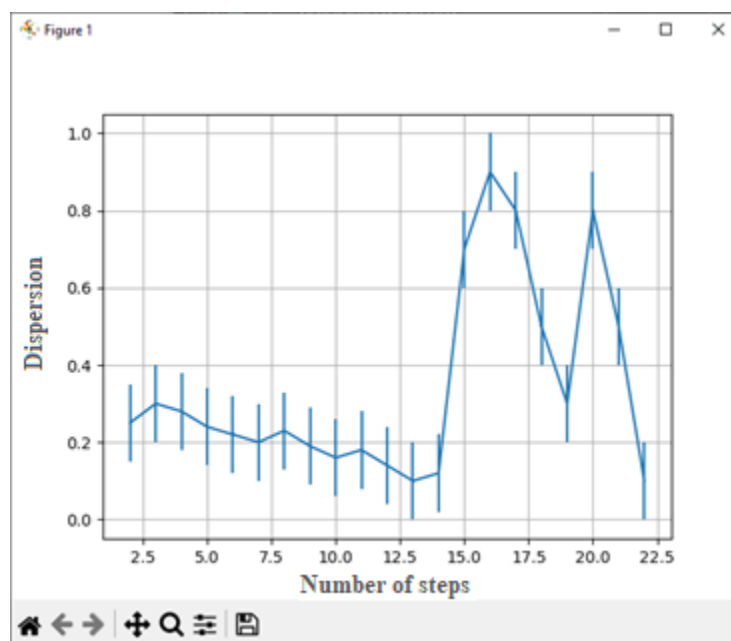


Figure 2. Dispersion of ANN training outcomes

Figure 1 demonstrates the situation in which the first player (the victim of a phishing attack), using the non-optimal behavior of the second player (the phisher) at the initial moment of time, "brings" the state of the system to "its" terminal surface. This terminal surface characterizes the phisher's loss of FR, since the cost of conducting a phishing attack did not produce a result. If the trajectory of the players coincides with the ray of balance, then this will correspond to the situation of equilibrium in the opposition of the players. In this case (which, however, is unlikely), the players, applying their optimal strategies, "move" along this ray. This "satisfies" both the "victim" and/or the defense side and the phisher at the same time. Accordingly, the costs of the victim (and/or the defense party) for leveling phishing are minimal. For example, it can be the high vigilance of a potential victim, as well as ignoring suspicious links and messages by mail and SMS. The costs of a phisher are also minimal. Since he, without resorting to costly phishing strategies, can simply implement a phishing mailing based on luck and chance. Complex and, accordingly, costly strategies are not used by the fisher.

If the trajectory of movement is under the beam of balance, then this will illustrate the situation when the first player (the victim and/or the side of the defense, for example, CCE) has an advantage in the ratio of parameters. That is, in this case they are in the preference set of the first player. In this case, the first player, applying his optimal strategy, will achieve his goal, namely, bringing the state of the system to "his" terminal surface.

As the graph on Figure 2 shows, the variance characterizing the spread of the experimental results shows that, starting from the value (the number of steps equal to the number of strategies in the payoff matrix) 2 and up to the value 14, the variance value is "acceptable", i.e. the spread of values is small. In addition, from a value of 21 it also becomes "acceptable". At values from 14 to 21, a zone of turbulence occurs. This gives grounds to determine the sample size (the number of strategies in the payoff matrix), which will allow using the trained ANN to make a fairly accurate prediction of the result of fighting phishing, namely, in this case, it is enough to limit the number of steps equal to 14.

Limitations. At this stage of the study, we limited ourselves to testing the simplest ANN in the form of a perceptron. This is a limitation and a certain disadvantage of the work. But with the accumulation of statistical materials, it is possible, if necessary, to create a more complex ANN. However, we note that we were primarily interested in solving the problem related to predicting the outcome of the confrontation of the parties during phishing attacks, and assessing the impact of the costs of the parties on protection (victims and/or protection of the CVB) and its overcoming (fisher).

4. CONCLUSION

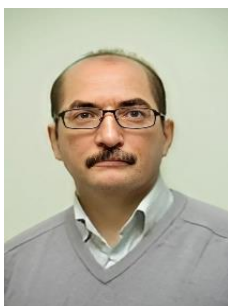
A dynamic model of countering phishing attacks on CCE and/or their clients is considered. The model, in contrast to similar ones that describe this problem, is built on the assumption that the dynamics of the states of the player-victim of phishing attacks and the player-intruder is set by means of a system of differential equations. Moreover, their solution makes it possible to form payoff matrices that are part of the training set for ANN. Such a collaboration of models, in our opinion, will make it possible to accurately build an anti-phishing strategy, minimizing the costs of both a potential victim of phishing attacks and the defense side when building a secure system of communication with clients, for example CCE. Besides, this approach makes it possible to predict the process of countering phishing in the context of costs for both parties using different strategies. It is shown that the controllability of the process of countering phishing attacks on market participants, for example, CC, can be described in terms of a game approach based on solving a bilinear differential game with several terminal surfaces. The novelty of the model lies in the fact that a solution has been found for a bilinear differential quality game with several terminal surfaces, which adequately reflects the essence of the problem under consideration. Solutions of bilinear differential games make it possible to form payoff matrices for ANNs, which makes it possible to predict the process of countering phishing. The results of a computational experiment are presented, during which various ratios of parameters describing the process of countering phishing attacks are taken into account.




REFERENCES

- [1] S. R. Routhu and R. P. Alwyn, "Routhu Srinidetection of phishing websites using an efficient feature-based machine learning framework," *Neural Computing and Applications*, no. 31, pp. 3851-3873, 2019, doi: 10.1007/s00521-017-3305-0.
- [2] B. B. Gupta, N. A. G. Arachchilage, and E. P. Kostas, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication Systems*, vol. 67, no. 5, pp. 247-267, 2018, doi: 10.1007/s11235-017-0334-z.
- [3] "Hackers stole more than \$40 million from the largest cryptocurrency exchange," [Online]. Available: <https://www.epravda.com.ua/rus/news/2019/05/8/647630/>. (accessed: Apr. 24, 2023).
- [4] C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, pp. 1-31, 2010, doi: 10.1145/1754393.1754395.
- [5] "Fake PrivatBank website revealed: Ukrainians are asked to be more careful," [Online]. Available: <https://www.unian.ua/economics/finance/viyavleno-falshiviy-sayt-privatbanku-ukrajinciv-prosyat-buti-oberezhnishimi-fotnovini-ukrajina-11489212.html>. (accessed: 21, Jul. 2021).
- [6] J. Chen, D. Lin and J. Wu, "Do cryptocurrency exchanges fake trading volumes? An empirical analysis of wash trading based on data mining," *Physica A: Statistical Mechanics and its Applications*, vol. 586, 126405, 2022, doi: 10.1016/j.physa.2021.126405.
- [7] A. Sharma, S. Ayush and D. Deepika, "Cryptocurrency: Perspectives, Applications, and Issues," in *Industry 4.0 Technologies for Business Excellence*, CRC Press, 2021, pp. 205-219.
- [8] A. F. Loe and E. A. Quaglia, "You shall not join: A measurement study of cryptocurrency peer-to-peer bootstrapping techniques," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2019, pp. 2231-2247, doi: 10.1145/3319535.3345649.
- [9] 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.
- [10] B. Harrison, E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails: How attention and elaboration protect against phishing," *Online Information Review*, vol. 40, no. 2, pp. 265-281, 2016, doi: 10.1108/OIR-04-2015-0106.
- [11] Y. A. Younis and M. Musbah, "A framework to protect against phishing attacks," in *Proceedings of the 6th International Conference on Engineering & MIS 2020*, Sep. 2020, pp. 1-6, doi: 10.1145/3410352.3410825.
- [12] A. Martin *et al.*, "A framework for predicting phishing websites using neural networks," *IJCSI International Journal of Computer Science Issues*, vol. 2, no. 8, 2011.
- [13] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," *Neural Computing and Applications*, no. 25, pp. 443-458, 2014, doi: 10.1007/s00521-013-1490-z.
- [14] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han, and J. Wang, "The application of a novel neural network in the detection of phishing websites," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-15, 2018, doi: 10.1007/s12652-018-0786-3.
- [15] W. Wei, Q. Ke, J. Nowak, M. Korytkowski, R. Scherer, and M. Woźniak, "Accurate and fast URL phishing detector: a convolutional neural network approach," *Computer Networks*, no. 178, p. 107275, 2020, doi: 10.1016/j.comnet.2020.107275.
- [16] A. C. Bahnsen, E. C. Bohorquez, S. Villegas, J. Varga, and F. A. González, "Classifying phishing URLs using recurrent neural networks," in *2017 APWG symposium on electronic crime research (eCrime)*, Apr. 2017, pp. 1-8, doi: 10.1109/ECRIME.2017.7945048.
- [17] W. Ali and A. A. Ahmed, "Hybrid intelligent phishing website prediction using deep neural networks with genetic algorithm-based feature selection and weighting," *IET Information Security*, vol. 13, no. 6, pp. 659-669, 2019, doi: 10.1049/iet-ifs.2019.0006.




- [18] F. Tchakounte, V. S. Nyassi, D. E. H. Danga, K. P. Udagepola, and M. Atemkeng, "A game theoretical model for anticipating email spear-phishing strategies," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 8, no. 30, pp. 1-24, 2021, doi: 10.4108/eai.26-5-2020.166354.
- [19] 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. 31, no. 1, pp. 92-133, 2017, doi: 10.1007/s10618-016-0459-9.
- [20] P. Sharma, B. Dash, and M. F. Ansari, "Anti-phishing techniques—a review of Cyber Defense Mechanisms," *IJARCCCE*, vol. 11, no. 7, pp. 153-160, 2022, doi: 10.17148/IJARCCCE.2022.11728.
- [21] J. Jansen and P. van Schaik, "The design and evaluation of a theory-based intervention to promote security behaviour against phishing," *International Journal of Human-Computer Studies*, no. 123, pp. 40-55, 2018, doi: 10.1016/j.ijhcs.2018.10.004.
- [22] H. Khan, M. Alam, S. Al-Kuwari, and Y. Faheem, "Offensive ai: unification of email generation through GPT-2 model with a game-theoretic approach for spear-phishing attacks," in *Competitive Advantage in the Digital Economy (CADE 2021)*, pp. 178-184, Jun. 2021, doi: 10.1049/icp.2021.2422.
- [23] V. Lakhno, V. Malyukov, N. Mazur, L. Kuzmenko, B. Akhmetov, and V. Hrebenuk, "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, doi: 10.15587/1729-4061.2020.194531.
- [24] S. A. Eint, T. Z. Chaw, and Y. Hayato, "A Survey of URL-based Phishing Detection," in *Department of Computer Science and Communication Engineering, Graduate School of Fundamental Science and Engineering, Waseda University, Tokyo, 159-8555*, 2019.
- [25] V. Lakhno, V. Malyukov, L. Parkhuts, V. Buriachok, B. Satzhanov, and A. Tabylov, "Funding model for port information system cyber security facilities with incomplete Hacker information available," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 13, pp. 4215-4225, 2018.

BIOGRAPHIES OF AUTHORS






Valery Lakhno    is a professor at the Department of Computer Systems, Networks and Cybersecurity at the National University of Life and Environmental Sciences of Ukraine, Ukraine. He holds a Ph.D. with a specialization in cybersecurity. His areas of research include mathematical modeling, security of computer systems and networks, and intrusion recognition. He has filed a number of patents and industrial designs for his innovative ideas in the field of cybersecurity. He can be contacted at email: lva964@nubip.edu.ua.






Volodimir Malyukov    is a professor at the Department of Computer Systems, Networks and Cybersecurity at the National University of Life and Environmental Sciences of Ukraine, Ukraine. He holds a Ph.D. with a specialization in the theory of multi-stage and differential games. His areas of research are mathematical modeling of economic and financial systems and their interaction. He has filed a number of patents on the creation of decision support systems in the field of investment to ensure cybersecurity. He can be contacted at email: volod.malyukov@gmail.com.






Inna Malyukova    is a leading analyst at the rating agency "Expert Rating", Ukraine. She is a Master of Banking with a specialization in the field of investments of banking structures and financial companies. She has developed a number of models for buying and selling cryptocurrencies, as well as models for managing financial flows of banks. She can be contacted at email: imalyukova82@gmail.com.






Bakhytzhon Akhmetov    Professor on the specialty 05.13.00- "Informatics, Computer Engineering and Management". Academician of the National Engineering Academy of the Republic of Kazakhstan. Passed all stages of a university career: from teacher to rector, scientific and pedagogical experience-45 years. Scientific interests-information and communication technologies, artificial intelligence, and cybersecurity. Publications-more than 400 articles, including 40 articles indexed in Scopus. Hirsch index in the Scopus database-7. Prepared 2 candidates of science, 15 Ph.Ds. Chairman of the National Scientific Council of the Republic of Kazakhstan on the priority Information, communication, and space technologies. Member of the editorial board of the journals "Information Protection", National Aviation University of Ukraine, Kyiv; "Ural Radio Engineering Journal", Ural Federal University named after the first President of Russia B.N. Yeltsin, Yekaterinburg. He can be contacted at email: bakhytzhon.akhmetov.54@mail.ru.



Zhuldyz Alimseitova    she is an associate professor at the Department of Cybersecurity, Information Processing, and Storage at Satpayev University of Kazakhstan. He holds a PhD in computer engineering and software engineering. Her research areas are information and cybersecurity, biometrics, pattern recognition, cryptography, and fiber-optic sensors. She can be contacted at email: zhuldyz_al@mail.ru.



Atkeldi Ogan    Doctoral student majoring in Information Security Systems at Satpayev University of Kazakhstan. Graduated from Satpayev University of Kazakhstan, majoring in computers, systems and networks, systems engineer. Master of Technical Sciences in Information Systems. His research areas are information and cybersecurity, biometrics, pattern recognition, cryptography, and fiber-optic sensors. He can be contacted at email: atkeldi@mail.ru.