Methods of information systems protection

UDC 004.056.55:519.8 **doi:** https://doi.org/10.20998/2522-9052.2026.1.12

Olha Hryshchuk[1], Ruslan Hryshchuk[2]

[1] National Defence University of Ukraine, Kyiv, Ukraine
[2] Military Academy (Odesa), Odesa, Ukraine

NON-TAYLOR DIFFERENTIAL GAMING PATTERN ECLIPSE ATTACK ON BLOCKCHAIN NODE

Abstract. **Relevance.** Information technologies of the 21st century have profoundly reshaped the global economy. As financial processes become increasingly digitalized, the role of traditional banking institutions as intermediaries is gradually diminishing. In this evolving landscape, blockchain technologies and cryptocurrencies have emerged as revolutionary tools, offering decentralized and secure alternatives to conventional financial systems. Cryptocurrencies, built on blockchain foundations, combine high reliability with robust protection against cyberattacks. However, both individual hackers and organized cybercriminal groups continue to target blockchain infrastructures – focusing not only on isolated nodes but also on entire networks and cryptocurrency wallets. Ensuring the resilience of blockchain technologies against such threats is therefore critical to safeguarding users' digital assets. Eclipse Attacks involve isolating a node to gain control over its information flows, posing a serious threat to network integrity. **The object of research.** This study introduces a differential game-theoretic model of Eclipse Attacks on blockchain nodes, formulated within a Markov chain framework. **The subject of the research.** The proposed model employs non-Taylor differential transformations developed by Academician G. Pukhov, enabling a more flexible analytical representation of attack dynamics. **The purpose of this paper**. The framework captures the strategic interaction between attacker and defender, offering a basis for assessing node security under adversarial conditions. **Research results.** As a result, the study provides a practical analytical toolkit for developing effective countermeasures against Eclipse Attacks and contributes to the broader discourse on cybersecurity in decentralized systems.

Keywords: blockchain node; differential game theory; cybersecurity; Eclipse Attack; security level; strategy.

Introduction

Relevance. The security of blockchain technologies is expected to become a significant global security challenge in the near future [1]. This is driven by both the increasing number of cryptocurrencies and the rapid growth of their market capitalization. Today, the most widely used cryptocurrencies include Bitcoin, Ethereum, Dash, Monero, Ripple, Ethereum Classic, Litecoin, NEM, Augur, and Maidsafecoin [2]. For instance, as of August 13, 2025, the price of one Bitcoin reached an all-time high of $123,500. The soaring capitalization of cryptocurrencies serves as a powerful incentive for the intensification of cybercrime. As a result, the number of cryptocurrency-related cyber incidents rose from 282 in 2023 to 303 in 2024, leading to the illicit appropriation of approximately $2.2 billion by cybercriminals [3]. It is highly likely that the number of such incidents will continue to grow in 2025 and 2026.

To identify vulnerabilities in blockchain technologies, cybercriminals employ a wide range of cyberattacks that vary in their methods, targets, and objects of impact [4]. At the network level, the most well-known attacks include the Routing Attack [5] and the 51% Attack [6]. At the blockchain node level, common attacks include Sybil Attacks [7], Denial of Service (DoS) [8], Timejacking Attacks [9], and Eclipse Attacks [10]. Given the growing diversity and increasing frequency of such attacks, protecting blockchain technologies requires a comprehensive approach. Today, legal, organizational, technical, administrative, and educational measures are actively applied to strengthen blockchain security. Scientific research also plays a critical role [11]. In particular, mathematical modeling [12] has become an essential tool for studying cyberattack mechanisms on blockchain systems [6–10], [13]. It enables researchers to analyze attack properties in depth and to develop effective countermeasures.

In this paper, the Eclipse Attack pattern is modeled using a differential game approach [14, 15]. This type of attack represents a significant threat to individual blockchain nodes within the network [16–18]. The foundation of the approach lies in game theory [19], which Satoshi Nakamoto was the first to apply in addressing the Byzantine Generals Problem. Consequently, game theory became the mathematical basis for the development of the Proof of Work consensus mechanism [20], which continues to be used for transaction validation.

An overview of scientific works. In recent years, there has been a significant increase in scientific research focused on the application of game theory to blockchain technologies. Among the most influential publications, [21] is considered fundamental. It provides a comprehensive review of the role and significance of game theory in blockchain at the current stage of scientific and technological development. In particular, [21] emphasizes that game-theoretic tools make it possible to analyze interactions between nodes within blockchain networks. For example, to model attacks such as Selfish Mining, Majority Attacks, and DoS Attacks, researchers have applied a variety of game-theoretic frameworks, including non-cooperative games, splitting games, mean-payoff games, stochastic games, sequential games, Stackelberg games, repeated games, extensive-form games, and coordination games. In practice, one of the most widely used approaches is the dynamic evolutionary game model [22], which enables the

simulation of node behavior within blockchain channels. This model incorporates factors such as the cost and success rate of cyberattacks, defense mechanisms, as well as cooperative and non-cooperative strategies during gameplay. The cyberdefence strategies derived from [22] can help blockchain nodes counter the most prevalent types of attacks. Furthermore, the model suggests that nodes can dynamically adapt their defense strategies to maximize security, depending on the tactics employed by cybercriminals. However, despite its advantages, the application of the dynamic evolutionary game model [22] remains limited and requires further validation. A similar challenge with verification also applies to the game-theoretic model described in [23].

Game theory has also been applied to the problem of modeling and distributing tokens among nodes in a blockchain network [24]. Using a game-theoretic approach, [24] developed a model of a self-sustaining token for blockchain applications. However, in focusing primarily on pricing issues for such tokens, the study placed less emphasis on modeling cyberattacks against blockchain nodes. In [25], a game-theoretic framework was proposed to formalize the outcomes – wins or losses – of players who deviate from the Proof of Work consensus mechanism [20]. This model provides a useful tool for analyzing the reliability of existing blockchain protocols.

One of the most recent dissertations on the application of a game-theoretic approach to studying blockchain stability is the work presented in [26]. In this study, game theory was applied to model player behavior strategies under the Ethereum Proof-of-Stake consensus mechanism, which relies on validators. As is well known, this mechanism is gradually replacing the traditional Proof of Work consensus based on mining [20]. The author of [26] demonstrated that if a participant's cyber defense deviates from the validation strategy prescribed by the Ethereum Proof-of-Stake protocol, the corresponding node is excluded from the blockchain and ultimately incurs losses. However, despite its theoretical and practical significance, the dissertation [26] does not address game-theoretic models of cyberattacks on blockchain nodes.

In [27], a game-theoretic model of a Ransom and Extortion Attack on Ethereum validators was developed. In this study, game theory was applied to analyze the behavior of cybercriminals seeking to coerce validators into paying a ransom for deploying smart contracts. In [28], game theory was for the first time employed to model cyberdefence strategies against Blockchain Sandwich Attacks. The practical contribution of [28] lies in identifying optimal behavioral strategies for both the market and participants during this type of attack. From the review of the above-mentioned studies [14–28], it can be concluded that none of them addressed the game-theoretic properties of an Eclipse Attack on a blockchain node using dedicated models.

Differential games, as a mathematical tool for analyzing conflict-driven processes, were first applied in [29] to model, simulate, and design networked token economies. The differential game model proposed in [29] allows players to maximize their payoff functions under conditions of uncertainty regarding cyber defense and attack strategies. This approach was further developed in the influential work [30]. In [31], the mathematical framework of differential games with stochastic dynamics was used to study player behavior strategies under uncertain conditions during cyberattacks on blockchain networks. The calculation of gains and losses for both cyber defense and cyberattack participants in [31] is based on the well-known Runge-Kutta algorithm. As a result, the differential game model proposed in [31], grounded in the Nash Equilibrium, enables the numerical estimation of gains and losses for each player during a simulated cyberattack. However, these estimates lose reliability if players deviate from the optimal strategies, which represents a limitation of the model [31]. Game theory is applied in [32] to develop a mathematical model of multidomain interaction; however, the model is conceptual and lacks practical implementation details.

For the first time, the Eclipse Attack on a blockchain node was modeled using differential game theory in [33], and a series of foundational works [34–37] established the corresponding mathematical framework. In [33], the probabilistic states of a blockchain node's reliability during an Eclipse Attack are formalized as a system of differential equations. The number of equations corresponds to the number of possible states of the blockchain node in a peer-to-peer network, which forms a Markov chain. It is worth emphasizing the following distinctions: study [34] is confined to the dependability evaluation of Bitcoin nodes under Eclipse Attack conditions; study [35] restricts its analysis to the dependability of nodes subjected to selfish mining attacks; study [36] extends the dependability assessment of Bitcoin nodes by incorporating both Eclipse and 51% attack scenarios. A holistic framework for selecting effective defense strategies against these cyber threats is presented in [37]. The above-cited studies also demonstrate that, depending on the strategies adopted by players for cyber defense or cyberattack, the value of the objective function – representing the real-time security state of the system – varies. From these results, it can be concluded that a key advantage of applying differential games in blockchain technologies is the ability to predict the future state of their security. The projected security state under cyberattack directly impacts the capitalization level of cryptocurrencies. However, neither in the studies analyzed in this paper nor in other widely cited publications have Eclipse Attack patterns on blockchain nodes been developed in an analytical form suitable for detailed security analysis.

Setting objectives. Therefore, in this study, building on the analysis of existing scientific literature, **the goal is** to develop an analytical model of the Eclipse Attack on a blockchain node using a differential game approach. This model will enable the assessment of node security under different player behavior strategies.

Research Methodology

Differential Game Basis: Main Definitions. In modeling the Eclipse Attack pattern on a blockchain node using differential game theory, this study adopts the following key concepts [14]: the participants in the conflict are defined as the cyber defense and cyberattack

players; the prescribed rules of behavior for these players are called strategies; the strategies are selected to optimize a specific criterion – the security level of the blockchain node – referred to as the payoff; the value of the game corresponds to the payoff at which the players simultaneously choose their optimal strategies; and the solution of the differential equations defines the trajectory of the game, representing the Eclipse Attack pattern on a blockchain node.

During the execution of an Eclipse Attack on a blockchain node, the interests of the players are inherently opposed. The cyber defense player aims to maximize the security of the node, while the cyberattack player seeks to minimize it. Under these conditions, the task of modeling the Eclipse Attack pattern assumes a differential game framework and is of a non-cooperative nature.

Verbal Description of the Eclipse Attack. As noted in [34], an Eclipse Attack begins when the cyberattacker initiates a connection between the targeted blockchain node and a false IP address selected from the routing table's IP pool. Such a connection can occur during a planned or forced restart of the node's software [34]. During a software restart, the victim node may connect to a malicious IP address, allowing the attacker to gain remote control and compromise the node. An increase in the number of blockchain nodes affected by Eclipse Attacks creates conditions that can facilitate more severe cyberattacks at the network level.

Formalized Description of the Eclipse Attack. To construct the Eclipse Attack graph, this study employs a semi-Markov process model [34]. This approach allows for the representation of a blockchain node's states while accounting for their probabilistic and temporal characteristics. As the node transitions between states under the influence of the players' chosen strategies, the sojourn times in different states may follow different probability distributions. This feature of semi-Markov processes ensures that the model accurately reflects the real dynamics occurring in a blockchain node during an Eclipse Attack.

The Eclipse Attack graph, constructed based on the semi-Markov process taking into account [34], is shown in Fig. 1.

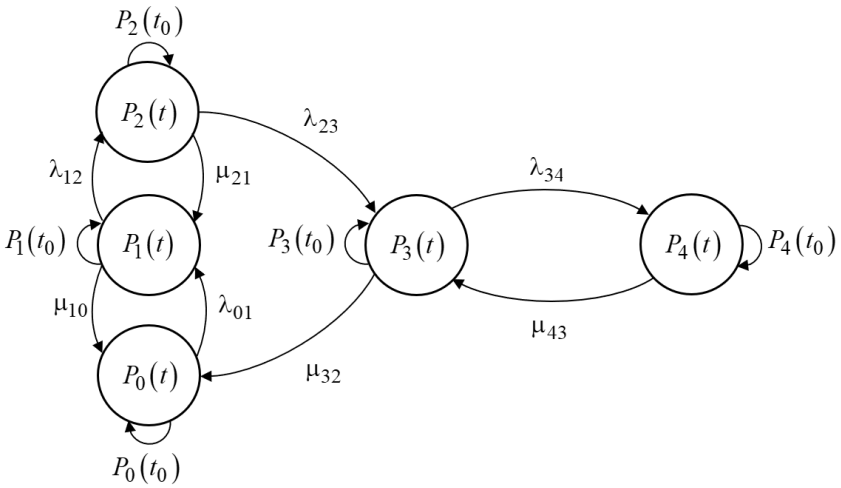

Fig. 1. Graph Model of Eclipse Attacks on a Blockchain Node Using a Semi-Markov Process

In Fig. 1 the following notations are used:

$P_0(t)$ – probability of a blockchain node being in a normal (secure) state, t – duration of Eclipse Attacks on a blockchain node, where t ∈ [t_0, T] , t_0 – start time, and T – cyberattack completion time, *s*;

$P_1(t)$ – probability of a player hacking the blockchain node routing table;

$P_2(t)$ – probability of a blockchain node restarting the routing table;

$P_3(t)$ – the probability of a remote connection by an attacking player to a blockchain node;

$P_4(t)$ – the probability of a blockchain node being administered by an attack player during which it is in an unprotected state;

λ_{01} – intensity of cyberattack on the blockchain node routing table with notification of incorrect IP addresses for reconnecting, s^{-1};

λ_{12} – intensity of a cyberattack aimed at initiating a restart of the blockchain node routing table, s^{-1};

λ_{23} – the intensity of a cyberattack that causes the routing table to restart and the blockchain node to connect to the wrong IP addresses, s^{-1};

λ_{34} – the intensity of a cyberattack that causes a blockchain node to connect to false IP addresses from a pool of IP addresses in a compromised routing table, s^{-1};

μ_{10} – intensity of detection and removal of messages with false IP addresses, s^{-1};

μ_{21} – intensity of cleaning the blockchain node routing table from the pool of false IP addresses, s^{-1};

μ_{32} – the intensity of restoring normal connections to legitimate IP addresses through maintenance activities, s^{-1};

μ_{43} – intensity of partial restoration of normal connections to legitimate IP addresses, s^{-1}.

Taking the above into account, the process of Eclipse Attacks on a blockchain node can be formally described by a system of differential equations based on the graph model (Fig. 1):

$$\begin{cases} \frac{dP_0(t)}{dt} = -\lambda_{01}P_0(t) + \mu_{10}P_1(t) + \mu_{32}P_3(t); \\ \frac{dP_1(t)}{dt} = -(\lambda_{12} + \mu_{10})P_1(t) + \lambda_{01}P_0(t) + \mu_{21}P_2(t); \\ \frac{dP_2(t)}{dt} = -(\lambda_{23} + \mu_{21})P_2(t) + \lambda_{12}P_1(t); \\ \frac{dP_3(t)}{dt} = -(\lambda_{34} + \mu_{32})P_3(t) + \lambda_{23}P_2(t) + \mu_{43}P_4(t); \\ \frac{dP_4(t)}{dt} = -\mu_{43}P_4(t) + \lambda_{34}P_3(t). \end{cases} \quad (1)$$

The system of differential equations (1) is valid under the initial conditions

$$P_0(t_0) = 1; P_1(t_0) = \ldots = P_4(t_0) = 0 \quad (2)$$

and rationing conditions

$$P_0(t) + P_1(t) + \ldots + P_4(t) = 1. \quad (3)$$

The intensity of cyberattacks and cyberdefences varies within

$$\begin{cases} 0 < \lambda_{ij} \le \lambda_{ij\,\max}; \\ 0 < \mu_{ji} \le \mu_{ji\,\max}; \end{cases}, \; i = 0,\ldots,3, \; j = 1,\ldots,4, \quad (4)$$

where $\lambda_{ij\,\max}$ – maximum intensity of cyberattack, and $\mu_{ji\,\max}$ – maximum intensity of cyber protection, while the blockchain node is in one of the states $P_0(t)$, …, $P_4(t)$.

The I - payoff for a broad class of differential games can be expressed as the sum of integral and terminal components [14]. To capture the dynamics of the Eclipse Attack process (1), the payoff should be formulated in an integral form, with integration performed along the game trajectory from its initial moment $t = t_0$ until its completion $t = T$. Let the integral payoff I for the developed pattern be the weighted average probability of the blockchain node remaining in a secure state. $P_0(t)$ under the influence of the Eclipse Attack. In general form it can be given by an expression of the form

$$I = \frac{1}{T}\int_{t_0}^{T} P_0(t)\,dt. \quad (5)$$

To determine optimal behavior in non-cooperative differential games, players can employ various types of strategies – guaranteeing strategies, Nash equilibrium strategies, and strategies derived from the concepts of "threats" and "counter-threats" [14]. A player's choice of strategy in a given differential game is guided by their objectives. When the players' goals are opposed, it is proposed to use the maximin principle as the strategy selection criterion. Under this principle, the first player – the cyber defense player – selects strategies μ_{ji}, which maximize the payoff (6) provided that it is minimized by the other player, i.e.

$$I(\mu_{ji}, \lambda_{ij}) = \max_{\mu_{ji} \in E_\mu} \min_{\lambda_{ij} \in E_\lambda} I, \quad (6)$$

where $I(\mu_{ji}, \lambda_{ij})$ – the payoff for the strategies μ_{ji} and λ_{ij} chosen by the players is defined in closed, bounded Euclidean spaces E_μ and E_λ, corresponding to the sets R_μ and R_λ that determine the possible strategies available to the players.

The second player – the cyberattack player – elects strategies λ_{ij} that minimize the payoff I, assuming it is being maximized by the first player, that is,

$$I(\mu_{ji}, \lambda_{ij}) = \min_{\lambda_{ij} \in E_\lambda} \max_{\mu_{ji} \in E_\mu} I. \quad (7)$$

If μ_{ji}^{opt} and λ_{ij}^{opt} are considered the optimal strategies for the allocation of the players available resources (4), then, under the condition that the following relation holds:

$$I^*(\mu_{ji}^{opt}, \lambda_{ij}^{opt}) = \\ = \max_{\mu_{ji} \in E_\mu} \min_{\lambda_{ij} \in E_\lambda} I = \min_{\lambda_{ij} \in E_\lambda} \max_{\mu_{ji} \in E_\mu} I, \quad (8)$$

there exists a saddle point in the game. The key property of a saddle point is that any deviation from the optimal strategy by one player results in a loss of payoff, assuming the other player continues to follow their optimal strategy [14], i.e.,

$$I^*(\mu_{ji}^{opt}, \lambda_{ij}) \le \max_{\mu_{ji} \in E_\mu} I(\mu_{ji}^{opt}, \lambda_{ij}); \quad (9)$$

$$I^*(\mu_{ji}, \lambda_{ij}^{opt}) \ge \min_{\lambda_{ij} \in E_\lambda} I(\mu_{ji}, \lambda_{ij}^{opt}). \quad (10)$$

The value of the game, or game price, is defined as the payoff $I^*(\mu_{ji}^{opt}, \lambda_{ij}^{opt})$ corresponding to the optimal strategies μ_{ji}^{opt} and λ_{ij}^{opt}. Taking into account the integral payoff (5), the game value (8) can be expressed in the form:

$$I^*(\mu_{ji}^{opt}, \lambda_{ij}^{opt}) = \max_{\mu_{ji} \in E_\mu} \min_{\lambda_{ij} \in E_\lambda} \left(\frac{1}{T}\int_{t_0}^{T} P_0(t)\,dt \right). \quad (11)$$

Non-Taylor Differential Transformers. From the model of the Eclipse Attack process (1) on a blockchain node, it is evident that constructing its differential game pattern requires processing a large volume of information in real time. Modern operational methods can be applied to address this challenge. Among the various available techniques, this study proposes using a modified method of differential transformations [38], specifically the non-Taylor differential-exponential transformations [39]. These transformations enable the real-time construction of accurate models of physical processes in the form of segments of exponential function series.

The general form of such transformations is expressed as follows [39]:

$$P(k) = \frac{H^k}{k!}\left[\frac{d^k P(t)}{dt^k}\right]_{t=0} \quad \overline{\bullet} \quad P(t) = \sum_{s=0}^{s=\infty} A_s e^{q_s t}, \quad (12)$$

where $P(k)$ – differential image of the original, which is a discrete function of an integer argument k, $k = 0,\ldots,n$;

$P(t)$ – the original, which is a continuous, infinitely differentiable and bounded function of a real argument with all its derivatives t;

H – a scale constant that has the dimension of the argument t and is chosen from the interval $0 \le t \le H$, on which the function is considered $P(t)$;

$\overline{\bullet}$ – symbol of correspondence between the original $P(t)$ and its differential image $P(k)$;

A_s, q_s – parameters of the approximating function.

Differential images $P(k)$ are called differential spectra, and the values of the function $P(t)$ at specific values of the argument k – discrete [39]. To the left of the symbol $\overline{\bullet}$ in transformations (13) is a direct transformation, which allows us to find the image $P(k)$ from the original $P(t)$, and to the right is an inverse transformation, which allows us to obtain the original $P(t)$ from the image $P(k)$ in the form of a series of exponential functions, where the coefficients A_s and the exponents q_s are to be determined.

To find unknown coefficients A_s and q_s let's write the spectral equation:

$$A_0 \text{ъ}(t) + \sum_{s=1}^{s=\infty} A_s q_s^k = \frac{k! P_0(k)}{H^k} = p_k, \quad p_k = \left[\frac{d^k P_0(t)}{dt^k}\right]_{t=0}. \quad (13)$$

By setting the values of the integer argument equal to $k =: 0,\ldots,3$ we obtain an algebraic system of equations

$$\begin{bmatrix} 1 & 1 \\ q_1 & q_2 \\ q_1^2 & q_2^2 \\ q_1^3 & q_2^3 \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} = \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \end{bmatrix} \quad (14)$$

The sought solution is the non-Taylor differential game pattern of Eclipse attacks on a blockchain node, taking into account the above, we will find it in the form of a segment of an exponential series of the form $P_0(t) = A_1 e^{q_1 t} + A_2 e^{q_2 t}$. At the same time, the right parts p_k we find based on the direct differential transformation [38].

Applying the direct differential transformation (12) to the system of differential equations (1) in the image domain, it will take the form

$$\begin{cases} P_0(k+1) = \frac{T}{k+1}\begin{pmatrix} -\lambda_{01}P_0(k) + \mu_{10}P_1(k) + \\ +\mu_{32}P_3(k) \end{pmatrix} \\ P_1(k+1) = \frac{T}{k+1}\begin{pmatrix} -(\lambda_{12}+\mu_{10})P_1(k) + \\ +\lambda_{01}P_0(k) + \mu_{21}P_2(k) \end{pmatrix}; \\ P_2(k+1) = \frac{T}{k+1}\left(-(\lambda_{23}+\mu_{21})P_2(k) + \lambda_{12}P_1(k)\right); \\ P_3(k+1) = \frac{T}{k+1}\begin{pmatrix} -(\lambda_{34}+\mu_{32})P_3(k) + \\ +\lambda_{23}P_2(k) + \mu_{43}P_4(k) \end{pmatrix}; \\ P_4(k+1) = \frac{T}{k+1}\left(-\mu_{43}P_4(k) + \lambda_{34}P_3(k)\right), \end{cases} \quad (15)$$

where the scaling constant H is chosen to be equal to the duration of the Eclipse Attack T, i.e. $H = T$. Taking into account (15), the discrete values for the probability of a Bitcoin node being in a normal (protected) state for different values of the integer argument k will be determined:

$$P_0(0) = \left[P_0(t=0)\right] = 1; \quad (16)$$

for $k = 0$: $$P_0(1) = -\lambda_{01} T; \quad (17)$$

for $k = 1$: $$P_0(2) = \frac{1}{2}\lambda_{01}(\lambda_{01} + \mu_{10})T^2; \quad (18)$$

for $k = 2$:

$$P_0(3) = -\frac{1}{6}\lambda_{01}\left((\lambda_{01}+\mu_{10})^2 + \lambda_{12}\mu_{10}\right)T^3. \quad (19)$$

Having found the right-hand sides (16)–(19), the algebraic system of equations (14) is given in the form

$$q_1 = \frac{P_0(3) - q_2^3 A_2}{P_0(2) - q_2^2 A_2}, \quad q_2 = \frac{P_0(1) - q_1 A_1}{P_0(0) - A_1},$$

$$A_1 = \frac{P_0(3) - q_2^3 A_2}{q_1^3}, \quad A_2 = \frac{P_0(1) - q_1 A_1}{q_2}$$

and solve it by iteration. So, taking $q_2 A_2 = 0$ at $T = 1c$ and taking into account (16)–(19), we obtain

$$q_1 = -\frac{1}{3}(\lambda_{01} + \mu_{10}), \quad q_2 = \frac{1}{2}\frac{\lambda_{01}}{\left(1 - \frac{9}{2}\left(\frac{\lambda_{01}}{\lambda_{01}+\mu_{10}}\right)\right)},$$

$$A_1 = \frac{9}{2}\left(\frac{\lambda_{01}}{\lambda_{01}+\mu_{10}}\right), \quad A_2 = 1 - \frac{9}{2}\left(\frac{\lambda_{01}}{\lambda_{01}+\mu_{10}}\right),$$

where $\lambda_{12} = 0$.

Thus, the non-Taylor differential game pattern Eclipse of the attack on the blockchain node $P_0(t)$, taking into account the found coefficients $\{(A_1, A_2); (q_1, q_2)\}$ from the system of algebraic equations (14) with an accuracy of λ_{12}, will be described by an analytical model of the form

$$P_0(t) = 4{,}5\cdot\left(\lambda_{01}/(\lambda_{01}+\mu_{10})\right)\times$$
$$\times\exp\left(-(\lambda_{01}+\mu_{10})t/3\right)+\left(1-\left(\lambda_{01}/(\lambda_{01}+\mu_{10})\right)\right)\times \quad (20)$$
$$\times\exp\left(\frac{1}{2}\frac{\lambda_{01}}{\left(1-4{,}5\cdot\left(\lambda_{01}/(\lambda_{01}+\mu_{10})\right)\right)}t\right).$$

The board (6) based on the direct differential transformation (13) taking into account the discretes (16)–(19) will take on the general form

$$I \approx \sum_{k=:0}^{k:=3}\frac{P_0(k)}{k+1} = 1-\frac{1}{2}\lambda_{01}T+\frac{1}{6}\lambda_{01}(\lambda_{01}+\mu_{10})T^2 - \quad (21)$$
$$-\frac{1}{24}\lambda_{01}\left((\lambda_{01}+\mu_{10})^2+\lambda_{12}\mu_{10}\right)T^3.$$

To find the optimal strategies μ_{ji}^{opt} and λ_{ij}^{opt} for allocating players' resources, we examine the payoff (21) at the extremum:

$$\begin{cases}\dfrac{\partial I\left(\mu_{ji}^{opt},\lambda_{ij}^{opt}\right)}{\partial\mu_{ji}^{opt}}=0;\\ \dfrac{\partial I\left(\mu_{ji}^{opt},\lambda_{ij}^{opt}\right)}{\partial\lambda_{ij}^{opt}}=0.\end{cases} \quad (22)$$

Finding the partial derivatives for each of the equations of system (22) reduced to a system of algebraic equations of the form

$$\begin{cases}\dfrac{T^2}{6}\lambda_{01}^{opt}-\dfrac{T^3}{12}\lambda_{01}^{opt}\left(\lambda_{01}^{opt}+\mu_{10}^{opt}\right)=0;\\ -\dfrac{1}{2}T+\dfrac{1}{6}T^2\left(2\lambda_{01}^{opt}+\mu_{10}^{opt}\right)=0;\end{cases}\Rightarrow\begin{cases}\mu_{10}^{opt}=\dfrac{1}{T};\\ \lambda_{01}^{opt}=\dfrac{1}{T},\end{cases} \quad (23)$$

if $\lambda_{12}^{opt}=0$.

Sufficient conditions for the existence of a saddle point $I\left(\mu_{10}^{opt},\lambda_{01}^{opt}\right)$ (8) are

$$\begin{cases}\dfrac{\partial^2 I\left(\mu_{10}^{opt},\lambda_{01}^{opt}\right)}{\partial\left(\mu_{10}^{opt}\right)^2}<0;\\ \dfrac{\partial^2 I\left(\mu_{10}^{opt},\lambda_{01}^{opt}\right)}{\partial\left(\lambda_{01}^{opt}\right)^2}>0.\end{cases} \quad (24)$$

Because

$$\begin{cases}\dfrac{\partial^2 I\left(\mu_{10}^{opt},\lambda_{01}^{opt}\right)}{\partial\left(\mu_{10}^{opt}\right)^2}=-\dfrac{T^3}{12}\lambda_{01}^{opt};\\ \dfrac{\partial^2 I\left(\mu_{10}^{opt},\lambda_{01}^{opt}\right)}{\partial\left(\lambda_{01}^{opt}\right)^2}=\dfrac{1}{3}T^2;\end{cases}\Rightarrow\begin{cases}-\dfrac{T^3}{12}\lambda_{01}^{opt}<0;\\ \dfrac{1}{3}T^2>0,\end{cases} \quad (25)$$

it can be stated that sufficient conditions (25) for the existence of a saddle point are satisfied. Based on this, players will choose optimal strategies (23) within the given constraints (4), i.e.

$$\mu_{10\ \max}^{opt}=\frac{1}{T};\quad \lambda_{01\ \min}^{opt}=\frac{1}{T}. \quad (26)$$

Taking into account (26), the price of the game, expressed as a function of two variables of the form (21), will be equal to

$$I^*\approx 0{,}667. \quad (27)$$

Thus, the maximum level of protection of a blockchain node from an Eclipse attack with the selected strategies (26) will not exceed the value of the game price (27).

Numerical Results and Impacts of Model Parameters. In order to verify the adequacy of the developed model (20) and assess the level of security of a blockchain node against Eclipse Attacks (21) depending on the strategies (4) chosen by the parties to the conflict, we present the modeling results in the Table 1.

Table 1 – **Dynamics of blockchain node security I under Eclipse Attack conditions ($\lambda_{12}^{opt}=0$, $T=1\,s$) analysis across diverse cyber defense μ_{10} and offense λ_{01} strategies.**

Model parameters		Optimal strategies	Optimal cyber defense strategy			Optimal cyber-attack strategy			Mixed strategies								
Cybersecurity intensity	μ_{10}, s^{-1}	1	1	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
Cyberattack intensity	λ_{01}, s^{-1}	1	1.25	1.5	1.75	1	1	1	1.25	1.5	1.75	1.75	1.25	1.5	1.5	1.75	1.25
Security level	I	0.667	0.58	0.484	0.376	0.643	0.656	0.664	0.57	0.5	0.398	0.417	0.58	0.496	0.496	0.412	0.583

To visualize the results (see table) and their further analysis, we present them in the form of a histogram (Fig. 2 a). Fig. 2 b–d present the probabilities of a Bitcoin node being in a protected state when chosen by players under the same player strategies (see Table 1).

Example Analysis and Discussions. From the analysis of the histogram (Fig. 2, a) it follows that the choice of strategies by players directly affects the level of security of the blockchain node during the Eclipse Attack**.** Thus, when players choose optimal cyber defense strategies $\mu_{10\ \max}^{opt}$ and cyberattack $\lambda_{01\ \min}^{opt}$ when $\lambda_{12}^{opt}=0$ and $T=1\,s$ the level of security of the blockchain node reaches its maximum and is expressed through the price of the game $I^*\approx 0.667$.

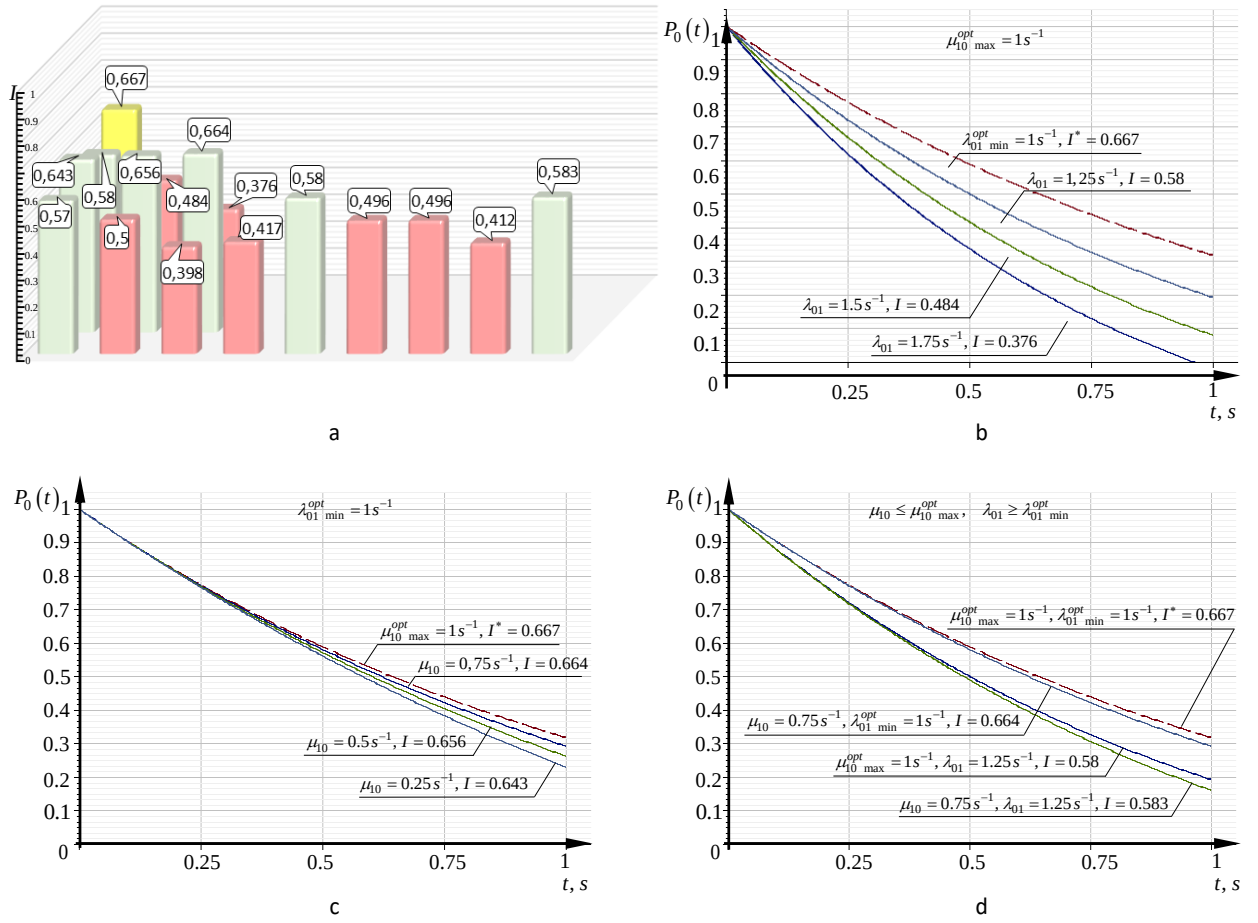

Fig. 2. Visualization of modeling results: a – histogram of the distribution of the level of security of a blockchain node during an Eclipse attack depending on the strategies chosen by the cyberattack and cyberdefence players; b – probability of a blockchain node being in a protected state when the cyberdefence player chooses the optimal strategy; c – probability of a blockchain node being in a protected state when the cyberattack player chooses the optimal strategy; d – probability of a blockchain node being in a protected state when the cyberdefence and cyberattack players choose mixed strategies

If the cyber defense player chooses the optimal strategy $\mu_{10}^{opt}{}_{\max}$ and the player's rejection of the cyberattack $\lambda_{01} \ge \lambda_{01}^{opt}{}_{\min}$ from its optimal strategy by no more than 25%, the node will remain protected, as the fee in the game will be no less than 0.58, that is, $0.58 \le I \le 0.667$. Under other strategies of the cyberattack player, the node is considered unprotected. When the cyberattack player chooses the optimal strategy $\lambda_{01}^{opt}{}_{\min}$ any cyber defense strategy within $\mu_{10} \le \mu_{10}^{opt}{}_{\max}$ do not significantly affect its security. At the same time, the fee I for such a deviation from the optimal strategy will not exceed the price of the game and will vary in the range $0.643 \le I \le 0.656$. Thus, if the cyberattack player follows his optimal strategy $\lambda_{01}^{opt}{}_{\min}$, saving its own resources, and the cyber defense player will choose an arbitrary strategy $\mu_{10} \le \mu_{10}^{opt}{}_{\max}$ the blockchain node will be secure.

Among the possible mixed strategies, the highest level of security of the blockchain node is achieved when the players deviate from the optimal strategies by no more than 25%. Therefore, the results obtained imply that it is not profitable for the players to deviate from their optimal strategies, which should have been proven (8).

Fig. 2b-2d illustrate that deviations from optimal strategies by the players result in a reduced probability of the blockchain node remaining in a secure state. The probability – and, correspondingly, the level of security – is highest when the players follow their optimal strategies.

Conclusion and Future Directions

In this work, a non-Taylor differential game pattern of an Eclipse Attack on a blockchain node is developed for the first time. The model is based on a modified differential transformation method, which provides an accurate operational approach for modeling complex dynamic processes. Unlike other known methods for constructing attack patterns on blockchain nodes, the proposed differential game approach enables:

(i) the analytical derivation of a non-Taylor differential game pattern of an Eclipse Attack and the investigation of its properties;

(ii) ii) the calculation of the guaranteed security level of a blockchain node under the influence of an Eclipse Attack;

(iii) and (iii) the determination of optimal behavior strategies for cyber defense and cyberattack players as they pursue their opposing objectives.

The numerical results presented confirm the adequacy of the developed non-Taylor differential game pattern, which serves as a foundation for selecting optimal cyber defense strategies against the most critical cyberattacks on blockchain technologies.

In future work, the developed pattern is intended to be used for evaluating a range of reliability metrics for blockchain nodes subjected to Eclipse Attacks. These metrics may include mean uptime, mean time to failure, mean recovery time following a cyberattack, availability factor, and other relevant indicators.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

REFERENCE

1. (2024), *The Global Risks Report 2024*, World Economic Forum, CH-1223, Cologny/Geneva, Switzerland, 124 p., available at: https://www.weforum.org/publications/global-risks-report-2024
2. Essien, N.P. and Okon, I.U. (2024), "Economic implications of cryptocurrency adoption: challenges and prospects", *Asia-Africa Journal of Academic Research and Review*, vol. 4, no. 1, pp. 100–118, available at: https://www.journals.iapaar.com/index.php/AAJARR/article/view/189
3. (2024), *Report: $2.2 billion stolen from crypto platforms in 2024, but hacked volumes stagnate toward year-end as DPRK slows activity post-July*, Chainalysis, available at: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025
4. Barj, S. and Youjil, A. (2024), "Blockchain and cryptocurrency security from a new layered perspective and a novel MITRE ATT&CK based approach for understanding cyberattacks and mitigating their impacts", *International Journal of Engineering Trends and Technology*, vol. 72, no. 4, pp. 1–14, doi: https://doi.org/10.14445/22315381/IJETT-V72I4P101
5. Hassija, V., Zeadally, S., Jain, I., Tahiliani, A., Chamola, V. and Gupta, S. (2021), "Framework for determining the suitability of blockchain: criteria and issues to consider", *Transactions on Emerging Telecommunications Technologies*, vol. 32, is. 10, e4334, doi: https://doi.org/10.1002/ett.4334
6. Aggarwal, S. and Kumar, N. (2021), "Attacks on blockchain", *Advances in Computers*, vol. 121, pp. 399–410, doi: https://doi.org/10.1016/bs.adcom.2020.08.020
7. Alachkar, K. and Gaastra, D. (2018), "Blockchain-based Sybil attack mitigation: a case study of the I2P network", *Semantic Scholar*, Corpus ID: 51696041, 22, pp.1–13, available at: https://www.os3.nl/_media/2017-2018/courses/rp2/p97_report.pdf
8. Chaganti, R., Boppana, R.V., Ravi, V. Munir, K., Almutairi, M. Rustam, F., Lee, E. and Ashraf, I. (2022), "A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges" *IEEE Access*, vol. 10, 96538–55, doi: https://doi.org/10.1109/ACCESS.2022.3205019
9. Aghili, S. (2024), *Leveraging Blockchain Technology*, CRC Press, Boca Raton, doi: https://doi.org/10.1201/9781003462033
10. Heilman, E., Kendler, A., Zohar, A. and Goldberg S. (2015), "Eclipse attacks on bitcoin's peer-to-peer network", *24th USENIX Security Symposium*, Washington, DC, USA, pp. 129–144, available at: https://dl.acm.org/doi/10.5555/2831143.2831152
11. Rico-Pena, J.J., Arguedas-Sanz, R. and Lopez-Martin, C. (2023), "Models used to characterise blockchain features: a systematic literature review and bibliometric analysis", *Technovation*, doi: https://doi.org/10.1016/j.technovation.2023.102711
12. Kumar, K.S,. Rajeswari, R., Vidyadhari, Ch. and Kumar, B.S. (2020), "Mathematical modeling approaches for blockchain technology", *IOP Conf. Ser. Mater. Sci. Eng*., vol. 981(2), pp. 1–8, doi: https://doi.org/10.1088/1757-899X/981/2/022001
13. Ahmad, R., Alsmadi, I., Alhamdani, W. and Tawalbeh, L. (2023), "Zero-day attack detection: a systematic literature review", *Artificial Intelligence Review*, vol. 56, pp. 10733–10811, doi: https://doi.org/10.1007/s10462-023-10437-z
14. Hryshchuk, R.V. (2010), *Teoretychni osnovy modeliuvannia protsesiv napadu na informatsyiu metodamy teoryi dyferentsialnykh ihor ta dyferentsialnykh peretvoren* (Ukrainian), Ruta, Zhytomyr, available at: https://surl.li/helyjo
15. Hryshchuk, R. (2021), "Example of differential transformations application in cybersecurity" *III Int. Sci. Pract. Conf. "Information Security and Information Technologies"*, Odesa, Ukraine, pp. 223–227, available at: https://ceur-ws.org/Vol-3200/paper31.pdf
16. Mufleh, A. (2019), *Bitcoin Eclipse Attack-Statistic Analysis on Selfish Mining and Double-Spending Attack*, Master Thesis. Johannes Kepler University Linz, Austria, 2019, available at: https://epub.jku.at/obvulihs/content/structure/3853668
17. Huang, K. (2023), "Chain security: nodes, algorithm, and network", *A Comprehensive Guide for Web3 Security*, Springer, pp. 31–60, doi: https://doi.org/10.1007/978-3-031-39288-7_2
18. Dholey, M.K. and Ganguly, A. (2022), "Major challenges and threats of blockchain technology", *Artificial Intelligence*, vol. 1695, pp. 96–108, doi: https://doi.org/10.1007/978-3-031-22485-0_10
19. Myerson, R.B. (1991), *Game Theory: Analysis of Conflict.*: Harvard University Press, Cambridge, MA, doi: https://doi.org/10.1002/MDE.4090130412
20. Gramoli, V. (2020), "From blockchain consensus back to Byzantine consensus", *Future Generation Computer Systems* , vol. 107, pp. 760–769, doi: https://doi.org/10.1016/j.future.2017.09.023
21. Liu, Z., Luong, N.C., Wang, W., Niyato, D., Wang, P., Liang, Y.-C. and Kim, D. I. (2019), "A survey on blockchain: a game theoretical perspective", *IEEE Access*, vol. 7, pp. 47615–47643, doi: https://doi.org/10.1109/ACCESS.2019.2909924
22. Zhang, P.Y., Li, C.X. and Zhou, M.C. (2020), "Game-theoretic modeling and stability analysis of blockchain channels", *2020 IEEE Int Conf Syst Man Cybern*., IEEE Inc., pp. 836–840, doi: https://doi.org/10.1109/SMC42975.2020.9282820
23. Tran, C.H., Le, D.T. and Huynh, T.H. (2021), "Game theory application resources management and distribution in blockchain network", *Int. J. of Network Security & Its Appl.,* vol. 13, no. 1, pp. 65–78, available at: https://ssrn.com/abstract=3791860
24. Udokwu, C. (2024), "Formalizing and simulating the token aspects of blockchain-based research collaboration platform using game theory", *Mathematics*, vol. 12, no. 10, pp. 1–19, doi: https://doi.org/10.20944/preprints202409.1808.v1
25. Zappalà, P., Belotti, M., Potop-Butucaru, M. and Secci, S. (2020), "Game theoretical framework for analyzing blockchains robustness", *Proc 34th Int.l Symp. on Distr. Comp.*, LIPIcs, vol. 49, pp. 1–3, doi: https://doi.org/10.4230/LIPIcs.DISC.2020.49

26. Pavloff, U. (2024), *A Game-Theoretic Approach to the Study of Blockchain's Robustness*, PhD Thesis, Paris-Saclay University, available at: https://pavloffulysse.com/manuscript-UlyssePavloff-EN.pdf
27. Bhudia, A., Cartwright, A., Hurley-Smith, D., Hurley-Smith, D. and Hernandez-Castro, J. (2023), "Game theoretic modelling of a ransom and extortion attack on Ethereum validators", *ARES'23: Proc 18th Int Conf Availability Reliability Security,* pp. 1–11, doi: https://doi.org/10.48550/arXiv.2308.00590
28. Liang, Y., Wang, X., Wu, Y.C., Fu, H. and Zhou, M. (2023), "Study on blockchain sandwich attack strategies based on mechanism design game theory", *Electronics*, vol. 12(4417), pp. 1–12, doi: https://doi.org/10.3390/electronics12214417
29. Zhang, Z. (2025), "Engineering token economy with system modeling", *arXiv*, doi; https://doi.org/10.48550/arXiv.1907.00899
30. Zhang, Z., Zargham, M. and Preciado, V.M. (2020), "On modeling blockchain-enabled economic networks as stochastic dynamical systems", *Applied Networks Science*, vol. 5, 19, pp. 1–24, doi: https://doi.org/10.1007/s41109-020-0254-9
31. Wang, H. and An, J. (2023), "Dynamic stochastic game-based security of edge computing based on blockchain*", Journal of Supercomputing,* vol. 79, pp. 15894–15926, doi: https://doi.org/10.1007/s11227-023-05289-x
32. Bazarnyi, S., Husak, Y., Voitko, T., Aliew, F. and Yevseiev, S. (2025), "Mathematical model of multi-domain interaction based on game theory", *Advanced Information Systems*, vol. 9, no. 3, pp. 22–31, doi: https://doi.org/10.20998/2522-9052.2025.3.03
33. Zhiyong, L., Shuyi, W., Weiwei, S., Jiahui, L. and Jianming, W. (2023), "Research on security situation awareness algorithm of Markov differential game blockchain model*", Journal of China Universities of Posts and Telecommunications,* vol. 30, no. 4, pp. 105–120, doi: https://doi.org/10.19682/j.cnki.1005-8885.2023.2020
34. Zhou, C., Xing, L., Liu, Q. and Wang, H. (2021), "Semi-Markov based dependability modeling of Bitcoin nodes under eclipse attacks and state-dependent mitigation*", Mathematical, Engineering and Management Sciences*, vol. 6, no. 2, pp. 480–92, doi: https://doi.org/10.33889/IJMEMS.2021.6.2.029
35. Zhou, C., Xing, L., Guo, J. and Liu, Q. (2022), "Bitcoin selfish mining dependability analysis", *International Journal of Mathematical, Engineering and Management Sciences*, vol. 7, no. 1, pp. 16–27, doi: https://doi.org/10.33889/IJMEMS.2022.7.1.002
36. Zhou, C., Xing, L., Liu, Q. and Li, Y. (2023), "System-level dependability analysis of Bitcoin under eclipse and 51% attack", *International Journal of Mathematical, Engineering and Management Sciences*, vol. 8, no. 4, pp. 547–59, doi: https://doi.org/10.33889/IJMEMS.2023.8.4.031
37. Zhou, C., Xing, L., Liu, Q. and Wang, H. (2023), "Effective selfish mining defense strategies to improve Bitcoin dependability", *Applied Sciences*, vol. 13(422), pp. 1–11, doi: https://doi.org/10.3390/app13010422
38. Pukhov, G.E. (1978), "Computational structure for solving differential equations by Taylor transformations", *Cybernetic and Systems Analysis*, vol. 14, pp. 383–390, doi: https://doi.org/10.1007/BF01074670
39. Pukhov, G.E. (1961), "Expansion formulas for differential transforms", *Cybernetic and Systems Analysis*, vol. 17, pp. 460–464, doi: https://doi.org/10.1007/BF01082476

Received (Надійшла) 30.09.2025
Acceptedforpublication (Прийнята до друку) 14.01.2026

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Грищук Ольга Михайлівна – доктор філософії, провідний науковий співробітник, Національний університет оборони України, Київ Україна;
Olha Hryshchuk – PhD, Leading Researcher, National Defence University of Ukraine, Kyiv, Ukraine;
e-mail: ol.hy@i.ua; ORCID Author ID: https://orcid.org/0000-0001-6957-4748.

Грищук Руслан Валентинович – доктор технічних наук, професор, заступник начальника Військової академії (м. Одеса), Одеса, Україна;
Ruslan Hryshchuk – Doctor of Technical Sciences, Professor, Deputy Commandant of the Military Academy (Odesa), Odesa, Ukraine.
e-mail: Prof.Hry@gmail.com; ORCID Author ID: https://orcid.org/0000-0001-9985-8477;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57192962493.

Нетейлорівська диференціально-ігрова модель Екліпс атаки на вузол блокчейну

О. М. Грищук, Р. В. Грищук

Анотація. Актуальність. Інформаційні технології XXI століття докорінно трансформували глобальну економіку. Із поступовою цифровізацією фінансових процесів роль традиційних банківських установ як посередників невпинно зменшується. У цьому новому середовищі технології блокчейну та криптовалюти постають як революційні інструменти, що забезпечують децентралізовану та захищену альтернативу класичним фінансовим системам. Криптовалюти, побудовані на основі блокчейну, поєднують високу надійність із стійкістю до кіберзагроз. Водночас як окремі хакери, так і організовані кіберзлочинні угруповання продовжують атакувати блокчейн-інфраструктуру. При цьому вони націлюються не лише на окремі вузли блокчейну, а й на цілі мережі та криптогаманці. Тому забезпечення стійкості блокчейн-технологій до таких загроз є критично важливим для захисту цифрових активів користувачів. Екліпс атаки, як один з різновидів кібератак у блокчейн-технологіях, передбачають ізоляцію вузла блокчейну з метою контролю над його інформаційними потоками, що становить серйозну загрозу цілісності мережі. **Об'єкт дослідження.** У роботі представлено диференціальну ігрову модель Екліпс атаки на вузол блокчейну, побудовану на основі марковських ланцюгів. **Предмет дослідження.** Запропонована модель базується на нетейлорівських диференціальних перетвореннях, розроблених академіком Г. Пуховим, що дозволяє гнучко аналізувати динаміку протікання Екліпс атаки. **Метою дослідження є** розроблення та дослідження нетейлорівської диференціально-ігрової моделі Екліпс атаки на вузол блокчейну. **Результати дослідження.** Розроблено аналітичний інструментарій, який може бути використаний для формування ефективних заходів протидії Екліпс атакам на вузли блокчейну.

Ключові слова: вузол блокчейну; теорія диференціальних ігор; кібербезпека; Екліпс атака; рівень захищеності; стратегія.