здійснені на будь-які інформаційно-комунікаційні системи незалежно від того, який рівень захисту у них присутній. З огляду на це більш значимим стає те, щоб найбільш швидко виявити кібератаки, зреагувати на них та поширити інформацію про такі випадки, щоб мати можливість мінімізувати їх можливу шкоду.

Отже, світ цифрових технологій, який швидкими темпами змінюється, вимагає того, щоб була сформована збалансована та ефективна національна система кібербезпеки, яка була б здатною до гнучкої адаптації до тих змін, які мають місце у безпековому середовищі. Таким чином, вона б гарантувала громадянам країни те, що національний сегмент кіберпростору буде безпечно функціонувати, а також передбачала б нові можливості цифровізації усіх сфер суспільного життя.

УДК 32.973.202 (004.8)

STRATEGY OF COUNTERING PHISHING ATTACKS ON THE CRYPTOCURRENCY EXCHANGE AS PART OF THE ENDLESS ANTAGONISTIC GAME SCHEME

Lakhno V.A.[1], Malyukov V.P.[1], Akhmetov B.S.[2], Alimseitova Zh.K.[3], Ogan A.[3]
National University of Life and Environmental Sciences of Ukraine[1], Kazakh National Pedagogical University named after Abai[2], Satpayev University[3]
[1]lva964@nubip.edu.ua, [1]volod.malyukov@gmail.com, [2]bakhytzhan.akhmetov.54@mail.ru, [3]zhuldyz_al@mail.ru, [3]atkeldi@mail.ru

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

Phishing has not bypassed such a popular type of commercial activity in recent years as trading in digital cryptocurrencies and, accordingly, affected online exchanges engaged in such transactions. With the development and growing popularity of exchanges engaged in trading digital cryptocurrencies, the problem of detecting and predicting the consequences of such attacks, including those based on phishing, remains relevant. In [1], examples of a number of fraudulent attacks aimed at the digital cryptocurrency exchange are considered. Information security specialists are looking for ways to ensure the interaction of all interested parties in order to counter fraud using phishing attack techniques and increase privacy for individual citizens and businesses. However, many

issues still need to be studied in more detail, in particular, relying on game-theoretic methods of analyzing situations that may arise as a result of a phishing attack. For example, when such an attack is aimed at customers of trading platforms engaged in the purchase and sale of digital cryptocurrencies. That is why in this publication we have tried to present our vision of this issue. The solution involved the apparatus of game theory, which made it possible to mathematically consider the situation with the counteraction of the party attacking with the help of phishing the participant of the trading session for the purchase and sale of digital cryptocurrencies.

That is why in this publication we have tried to present our vision of this issue. The solution involved the apparatus of game theory, which made it possible to mathematically consider the situation with the counteraction of the party attacking with the help of phishing the participant of the trading session for the purchase and sale of digital cryptocurrencies.

In the course of research, a mathematical model has been developed for the computational core of the decision support system made during the exchange's trading session on the sale and purchase of digital cryptocurrencies. The model promotes the adoption of rational decisions to ensure the information security of players who may face the threat of a phishing attack against them. The model is developed on the basis of an endless antagonistic game and is designed to find optimal strategies for players. The solution of such a problem contributes to the analytical search not only for the meaning of the game for the interested party, but also makes it possible to find the characteristics of the degree of risk of achieving the goal by players when they use optimal mixed strategies. In particular, such a solution contributes to the analysis of the situation with the counteraction of the party attacking with the help of phishing the participant of the trading session on the purchase and sale of digital cryptocurrencies.

Computational experiments were conducted using the Anaconda distribution kit (PyChar Professional programming environment), which made it possible to visualize the results of the game and will be useful for analysts dealing with information security issues of trading platforms specializing in buying and selling digital cryptocurrencies and countering such threats as phishing attacks.

References

1. Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., ... & Xu, G. (2020). Characterizing cryptocurrency exchange scams. Computers & Security, 98, 101993.