DOI 10.31891/2307-5732-2024-341-5-73
УДК 004.056

PETLIAK NATALIIA
Khmelnytskyi National University
https://orcid.org/0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua
BEZKOROVALNYI YAROSLAV
Khmelnytskyi National University
e-mail: bezkorovalnyiiao@khmnu.edu.ua
KUPCHYK NATALIIA
Khmelnytskyi National University
e-mail: nataliiakupchyk@khmnu.edu.ua

ANALYSIS OF MODERN METHODS OF DETECTION OF PHISHING E-MAILS

Phishing attacks are one of the common threats to modern cyber security. The most common method fraudsters use to send fake messages to collect data is phishing emails. However, with the development of technology and artificial intelligence, the number and complexity of phishing attacks are increasing, making detecting them difficult. The article discusses traditional and modern methods of combating phishing, particularly blocklists and signature methods, and the latest machine and deep learning approaches. The analysis of the latest research made it possible to develop a generalised algorithm (fig. 2) for the implementation of the phishing email detection system, which consists of the following steps: data collection, data pre-processing, feature selection, modelling, email classification, model updating, blocking and notification/ Machine learning makes it possible to analyse large volumes of data and detect hidden patterns, which makes these methods effective for automatically blocking phishing emails. Convolutional and recurrent neural networks are also used to analyse the text of phishing messages at the level of words and phrases. Special attention is paid to developing natural language processing methods that help better understand the context of letters and detect anomalies. Deep models allow for extracting valuable features without pre-processing the data, making them practical for detecting new attacks. The implementation of machine and deep learning methods significantly increases the effectiveness of detecting phishing emails. However, further research is needed to improve and realise the models' full potential. It is necessary to create models that can independently adapt to new threats without manual intervention, analysing new patterns and strategies of attackers. This will ensure a more effective fight against phishing threats in the rapidly changing digital environment.

Keywords: phishing, social engineering, Large Language Model, machine learning.

ПЕТЛЯК НАТАЛІЯ
Хмельницький національний університет
БЕЗКОРОВАЛЬНИЙ ЯРОСЛАВ
Хмельницький національний університет
КУПЧИК НАТАЛІЯ
Хмельницький національний університет

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ВИЯВЛЕННЯ ФІШИНГОВИХ ЕЛЕКТРОННИХ ЛИСТІВ

Фішингові атаки є однією з поширених загроз сучасній кібербезпеці. Найпоширеніший метод, який використовують шахраї для надсилання фальшивих повідомлень для збору даних, – це фішингові електронні листи. Однак із розвитком технологій і штучного інтелекту кількість і складність фішингових атак зростає, що ускладнює їх виявлення. У роботі наведено аналіз фішингових атак, етапи їх еволюції та основні методи захисту. Також розглянуто традиційні та сучасні методи боротьби з фішингом, зокрема списки блоків і сигнатурні методиу, алгоритми машинного та глибокого навчання. Машинне навчання дає змогу аналізувати великі обсяги даних і виявляти приховані шаблони, що робить метод ефективними для автоматичного блокування фішингових електронних листів. Згорткові та рекурентні нейронні мережі також використовуються для аналізу тексту фішингових повідомлень на рівні слів і фраз. Особлива увага приділяється розробці методів обробки природної мови, які допомагають краще розуміти контекст літер і виявляти аномалії. Глибокі моделі дозволяють отримувати цінні функції без попередньої обробки даних, що робить їх практичними для виявлення нових атак. Проаналізовано основні недоліки та перспективу подальших досліджень у контексті кіберзахисту.

Ключові слова: фішинг, соціальна інженерія, Large Language Model, машинне навчання.

Introduction

Phishing attacks are one of the common cybersecurity threats in today's digital world. They attack individual users, large organisations, and governments, making them a universal problem. The primary goal of such attacks is to obtain sensitive information such as passwords, credit card numbers, or personal information by impersonating the attacker as a trusted source. The nature of phishing attacks is constantly evolving, and their complexity is growing, which creates additional challenges for security systems and prompts the development of new, more sophisticated protection methods. Among the widespread forms, it is possible to single out phishing attacks via e-mail [1-2]. This method involves scammers sending fake emails that look legitimate to trick the victim into providing sensitive information or clicking on a malicious link. Along with this, other forms are common, such as spear phishing (targeted attacks on specific individuals or organisations), vishing (phishing via phone calls) and smishing (phishing via SMS).

With the development of digital technologies and Internet services, the number and complexity of phishing attacks have increased dramatically [3-4]. And the remote working mode has increased the dependence on e-mail and other online services. This has created additional opportunities for attackers who have adapted their methods to attack less secure networks and users who need more cybersecurity training.

Phishing is a form of social engineering in which criminals manipulate users to force them to reveal confidential information [5-6]. According to the Anti-Phishing Working Group (APWG) report, phishing attacks increased significantly in 2023, reaching more than 1.2 million in the second quarter. The main target of phishing attacks remains the financial sector, which accounts for more than 23% of all cases [7]. Other vital industries such as healthcare, e-commerce and education face this threat. The problem is exacerbated by social engineering, which is often the first step in more sophisticated cybercrimes, such as infrastructure attacks or malware distribution.

Especially dangerous is the emergence of so-called "black" models of large language models that automate the creation of phishing messages. These models generate high-quality, personalised messages that are difficult to distinguish from legitimate emails. Criminals use them to create campaigns of mass phishing attacks, which significantly complicates the process of their detection and blocking.

Detecting phishing attacks is essential for keeping users and organisations safe. Classic anti-phishing methods include blocklists and signature methods. Blocklists allow you to capture suspicious domains or IP addresses used in previous attacks. However, this method has limitations due to the dynamic nature of phishing attacks. Fraudsters are constantly creating new URLs or changing minor details to bypass blocklists. The signature-based method also has drawbacks, as successful detection requires prior knowledge of attack patterns, and phishing often has new variations.

Traditional approaches are replaced by machine learning and deep learning methods, which demonstrate significant effectiveness in detecting phishing attacks. Machine learning algorithms can analyse large volumes of data, identify hidden patterns, and make predictions based on this data. Such methods allow the modelling of complex defence systems that can automatically adapt to new attacks, minimising human involvement. For example, machine learning algorithms can be trained on large datasets of phishing emails, identifying essential characteristics for their identification. This allows you to create effective systems for automatically blocking phishing messages before they are delivered to the user.

Unlike machine learning, deep learning techniques such as convolutional neural networks or recurrent neural networks can independently extract useful features from raw data without needing to pre-select features. This makes them practical for phishing detection and text classification tasks. Deep neural networks have demonstrated performance in various natural language processing tasks, including sentiment analysis, text categorisation, and message classification. However, these methods have several disadvantages, including the requirements for significant computing resources and difficulty explaining the decisions made.

Classification of methods for detecting phishing emails

Different methods of detecting phishing e-mails (fig. 1) have been developed to combat these threats, and each of them is based on different theoretical aspects and approaches that allow not only the identification of the danger but also the protection of the system from potential attacks.

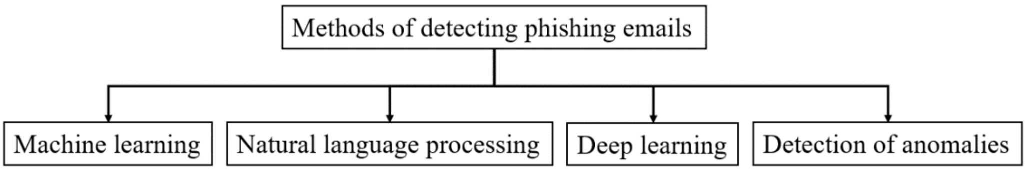
Methods of detecting phishing emails
Machine learning
Natural language processing
Deep learning
Detection of anomalies

Fig. 1. Methods of detecting phishing emails

Machine learning is one of the main techniques widely used to detect phishing emails. The theoretical basis of machine learning is that the system can learn from previously collected data and model the behaviour of phishing attacks, using this data to predict new threats. Algorithms such as logistic regression, support vector machines, random forests and neural networks are used. Logistic regression is a classic two-class classification approach that predicts the probability that a given email is phishing. Support vector machines determine the optimal boundaries between classes, ensuring high accuracy in classifying phishing emails. Random Forest is an ensemble learning method that creates multiple tree-based solutions that increase robustness to variations in the data. Neural networks make it possible to effectively work with sequential text data, revealing hidden dependencies between words in the text of phishing emails. The main advantage of machine learning is the ability to automatically improve its results with new data, which allows the creation of dynamic detection systems that adapt to new types of attacks.

Natural language processing (NLP) is one of the techniques for detecting phishing emails because the primary information is in the text. The theoretical basis of NLP is to transform textual data into formats suitable for analysis and to detect potentially harmful patterns in the content of emails. NLP steps include tokenisation, stemming, and vectorisation. During tokenisation, the text is split into separate words or phrases. Stemming allows you to simplify words to their base form to improve text analysis. Text vectorisation using Bag of Words or Term Frequency-Inverse Document Frequency methods will enable you to convert text into numerical vectors for machine analysis. Modern NLP models, such as Bidirectional Encoder Representations from Transformers and Generative Pre-trained Transformer, provide contextual embedding of words, which allows the detection of more complex semantic relationships and phrases characteristic of phishing attacks. Detection of anomalies in the text can also be used to identify elements that are not characteristic of routine correspondence, which may indicate phishing.

Deep learning allows you to create robust models to detect complex phishing patterns using large amounts of data. Deep learning models will enable the recognition of text and understanding of its context by studying interactions between words and their positions in the text. Fundamental in this context are models that allow embedding words' semantic and contextual meanings into vectors, making it possible to analyse individual words and their relationships in the text. With the ability to process large volumes of data and discover hidden connections, deep learning can help identify new and previously unknown phishing schemes.

Approaches based on detecting anomalies assume that phishing emails differ from ordinary emails by specific characteristics. Using statistical methods or machine learning algorithms allows you to analyse the typical behaviour of postal communications and determine deviations from this behaviour. For example, distance-based methods such as K-nearest neighbours help measure the similarity between a new email and already-known phishing patterns. Density-based methods, in turn, allow the detection of groups of anomalous emails that may indicate a massive phishing attack. Methods based on reconstruction (for example, autoencoders) study standard email patterns and detect those that differ from them.

One of the key theoretical aspects is the development of functions used to train models. Detecting phishing emails requires picking suitable email characteristics, such as text content, metadata, sender information, URLs, and behavioural data. Analysing textual content helps identify suspicious patterns or words typical of phishing messages. Analysis of metadata and email headers allows you to check the time of sending/receiving the email and the history of interactions with the sender, which can help detect suspicious activity. Analysing URLs in the text and studying the reputation of domains allows you to detect fake or malicious links.

Various theoretical approaches to detecting phishing e-mails allow the creation of sophisticated and effective systems to combat this threat. Each of the approaches has its advantages and limitations. Still, their combination will enable you to achieve the best results in detecting phishing and ensuring cyber security at the appropriate level.

Analysis of the latest research on methods of detecting phishing emails

The authors [8] suggest using machine learning models to classify phishing e-mails, dividing them into those generated by humans and by the Large Language Model (LLM). The research collected a dataset of thousands of human-generated phishing emails and thousands more emails created using WormGPT. Several machine learning models, such as neural networks, SVM, logistic regression, and others, have been used. However, if attackers begin to actively change the styles of creating phishing emails or use other LLMs to generate attacks, the effectiveness of the models may decrease. Since phishing attack tactics constantly change, the model will need regular updates and retraining to remain effective. The models have yet to be tested in open real-world conditions or conflict situations where attackers can actively counter defence mechanisms.

The study [9] presents an approach to detecting phishing e-mails using a deep learning model using an advanced convolutional neural network. The proposed model analyses phishing emails at multiple levels, focusing on the email header, body, character, and word levels. The model uses an attention mechanism that allows you to prioritise more critical information in the letter's structure. The study highlights the limitations of traditional phishing detection methods, such as blocklist mechanisms and classical machine learning algorithms, which require manual development of features and cannot adapt to the specifics of phishing emails. The model was tested on an unbalanced data set representing real-world proportions of phishing and legitimate emails. The model's results demonstrate its ability to recognise phishing emails more effectively than previous methods. A system architecture, including a data flow diagram and an entity-relationship model, is developed to represent the e-mail discovery and management process. The authors acknowledge the need for further improvement, particularly in cases where phishing emails do not contain critical headers.

The research in [10] involves developing and implementing a new model for detecting phishing e-mails based on recurrent convolutional neural networks using multi-level vectors and an attention mechanism. The study's uniqueness is that it analyses the structure of e-mails and considers both the header and the body of the letter at the level of characters and words. This allows for more accurate detection of phishing attacks, especially in the part of the email that most often contains fraudulent elements. An unbalanced database containing realistic proportions of phishing and legitimate emails was used to evaluate the proposed model's effectiveness. In addition, the study analyses existing technologies such as sender and link blocklists but notes that their effectiveness depends on the relevance and completeness of such lists. The authors highlight the growing threat of phishing attacks and emphasise the importance of automated tools based on machine learning and neural networks to counter these threats. The proposed model with multilevel vectors and an attention mechanism requires significant computing power for learning and working in real-time.

The work [11] systematically analyses NLP and machine learning methods. The study compares machine learning methods, including the Naive Bayesian classifier and logistic regression, focusing on their accuracy, reliability, and performance. Considerable attention is paid to the importance of data preprocessing, mainly cleaning, tokenisation, and removal of stop words, improving text analysis quality. A unique approach is also the analysis of URL characteristics to detect phishing sites, such as link length, presence of memorable characters and anomalies in the domain structure. This study offers an in-depth comparative analysis of existing methods and points to ways to improve the accuracy and effectiveness of phishing protection. Pre-processing of the data, including tokenisation and removal of stop words, can lead to the loss of important information, which can reduce the accuracy of the models.

Article [12] describes developing a system that detects and blocks phishing e-mails in real time using machine learning. The system recognises the difference between legitimate and malicious emails by analysing various characteristics such as email content, headers and attachments. This approach protects users from phishing attacks and prevents the spread of malware and other threats. For example, the system can detect phishing emails imitating bank communications by analysing suspicious elements such as the sender's email address or requests for personal information. In addition, it protects against malicious attachments such as viruses or ransomware, thereby protecting users' devices from compromise and the spread of threats. Thanks to the model's ability to adapt and constantly improve through analysing new data, the system remains effective against the latest phishing tactics.

The authors of [13] suggest improving the detection system of phishing e-mails using combined machine learning algorithms. The study presents an approach combining supervised and unsupervised machine learning algorithms to analyse email properties and user behaviour to detect subtle signs of phishing. The system analyses email content, sender reputation, and behaviour patterns. It uses advanced natural language processing and pattern recognition algorithms to evaluate email content, URLs, and information from QR codes. The integration of these methods allows to improve the accuracy of detection of phishing attacks and reduce the number of false positive results compared to existing detection techniques. The study also highlights the importance of adapting to new phishing tactics, such as dynamic content loading and URL obfuscation. It suggests a comprehensive approach that includes monitoring login activity, scanning QR codes and URLs, and in-depth email content analysis. This extensive method increases email security and provides a proactive approach to cybersecurity, making it a valuable tool for protecting against phishing attacks.

The authors of [14] created an interpreted AI-based platform for real-time detection of phishing emails, using the most extensive available public data sets to train models, significantly improving their generalisation ability. The paper proposes a methodology for combining several data sets to increase the effectiveness of detecting different phishing emails.

Research [15] aims to solve phishing attacks by developing a hybrid approach combining machine and deep learning methods. Using a genetic algorithm to optimise feature selection allows the model to identify better features, which increases its performance. The proposed approach was evaluated on a dataset of 1,173 records emphasising writing letters with Arabic content.

Research [16] focuses on increasing the effectiveness of detecting phishing e-mails using ensemble learning, which combines different machine learning methods. The proposed model demonstrates an increase in accuracy compared to traditional approaches to classification, thanks to the combination of several algorithms, which allows for better detection of details and patterns characteristic of phishing attacks. A stack method combines SVM, XGBoost and logistic regression to optimise the classification.

Algorithm for detecting phishing emails

The analysis of the latest research made it possible to develop a generalised algorithm (fig. 2) for the implementation of the phishing email detection system, which consists of the following steps: data collection, data pre-processing, feature selection, modelling, email classification, model updating, blocking and notification.

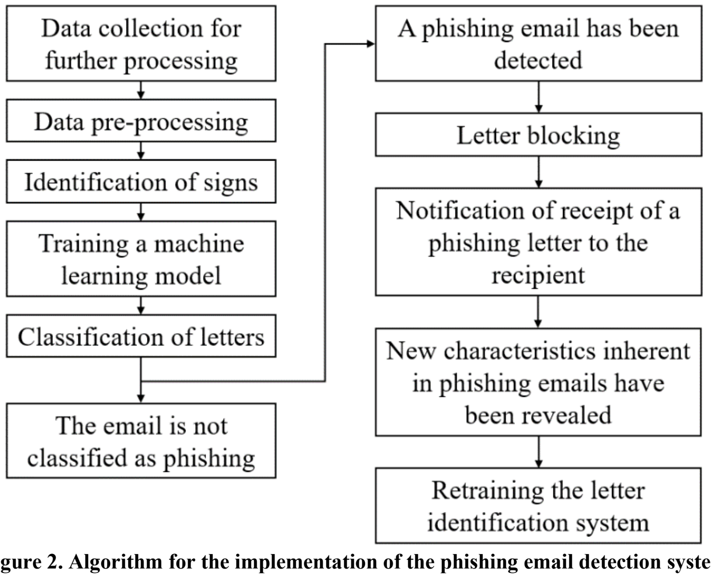
Data collection for further processing
Data pre-processing
Identification of signs
Training a machine learning model
Classification of letters
The email is not classified as phishing
A phishing email has been detected
Letter blocking
Notification of receipt of a phishing letter to the recipient
New characteristics inherent in phishing emails have been revealed
Retraining the letter identification system

Figure 2. Algorithm for the implementation of the phishing email detection system

During the collection, the data necessary for identifying the phishing letter is selected; in particular, such data includes letter headers, attachments, the sender's address, the body of the letter, and other parameters. The next stage is data collection, which involves providing legitimate and phishing emails. Data pre-processing consists of removing unnecessary characters, HTML tags, and special characters that do not carry significant information, breaking the text into separate words or symbols, removing words that do not have meaningful information, and reducing words to their primary form to reduce data dimensionality. Identifying the signs of phishing emails begins with content analysis, which examines keywords and specific phrases frequently used by attackers. These can be urgent requests for action or threats to block the account. Next, the URLs are checked for anomalies such as length, suspicious characters, or obfuscation. The metadata of the letter is also analysed, particularly the headers, where the sender and the domain's reputation are evaluated. A critical component is the analysis of attachments for malware or suspicious file types. At the simulation stage, appropriate machine learning models such as naive Bayesian classifier, logistic regression, recurrent neural networks, deep neural networks with an attention mechanism, or convolutional neural networks are selected, which allow text analysis at the character and word level. The model is trained on labelled data containing both phishing and legitimate emails. After training, its performance is evaluated by metrics such as accuracy, completeness, specificity, and F1-measure. When classifying new mail, the incoming mail undergoes the same preprocessing and feature extraction procedure. The model classifies the email as phishing or legitimate based on the features it obtains. As phishing attack tactics change, the model is tested for effectiveness and needs to be periodically retrained on new data to stay relevant, considering new writing styles or text generation methods. If the email is recognised as phishing, it is automatically blocked or moved to the "Spam" folder. The user receives a notification about a potential threat with recommendations for caution or further actions. For example, the algorithm can integrate with other systems to check senders and URLs using blocklists or reputation databases. In addition, the user's behaviour during interaction with the letter is analysed to detect potentially dangerous actions.

Conclusions

The implementation of machine and deep learning methods significantly increases the effectiveness of detecting phishing emails. However, further research is needed to improve and realise the models' full potential. It is necessary to create models that can independently adapt to new threats without manual intervention, analysing new patterns and strategies of attackers. This will ensure a more effective fight against phishing threats in the rapidly changing digital environment.

Література

1. Most Common Types of Phishing Attacks in 2024. URL: https://www.upguard.com/blog/types-of-phishing-attacks (дата звернення 2.09.2024)
2. Phishing Attacks: Statistics and Examples. URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing (дата звернення 2.09.2024)
3. Тенденції у розвитку фішингу та протидія йому. URL: https://my-itspecialist.com/trends-in-phishing-development-and-countermeasures (дата звернення 3.09.2024)
4. Trends in Cyber Challenges and Solutions 2024. URL: https://www.h-x.technology/blog/trends-cyber-challenges-solutions-2024 (дата звернення 4.09.2024)
5. Avoiding Social Engineering and Phishing Attacks. URL: https://www.penncommunitybank.com/wp-content/uploads/2021/06/Avoiding-Social-Engineering-and-Phishing-Attacks.pdf (дата звернення 4.09.2024)
6. Understanding Social Engineering Tactics: 8 Attacks to Watch Out For. URL: https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for (дата звернення 9.09.2024)
7. Phishing activity trends report. URL: https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf (дата звернення 9.09.2024)
8. Francesco Greco, Giuseppe Desolda, Andrea Esposito, Alessandro Carelli. David versus Goliath: Can Machine Learning Detect LLM-Generated Text? A Case Study in the Detection of Phishing Emails, ITASEC: The Italian Conference on CyberSecurity, Italy, Vol. 3731, 2024.
9. P. R. Uyyala. Phishing email detection using CNN, Journal of Engineering and Technology Management, Vol. 72, 2024, pp. 1046-1051.
10. S. A.Nabi, G. Srija, G. Madhuri, M. R. Reddy, C. Jashuva, Phishing email detection using improved RCNN with multilevel. International Journal For advanced research in science & technology, Vol. 13, No. 7, 2023, pp. 63–69.
11. J.Keerthika, A. Adisvara, S. Akash, B. Jayanesh, T. Arul Prakash, E-mail spam detection and phishing link detection using machine learning, Advances in Computational Intelligence in Materials Science, 2023, pp. 47-53, doi: 10.53759/acims/978-9914-9946-9-8_9.
12. Jude Osamor et al, Real-Time Detection of Phishing Emails Using XG Boost Machine Learning Technique, International Conference on Information Technologies and Smart Systems, India, 2024.
13. G. B. Sambare, S. B. Galande, S. Kale, P. Nehete, V. Jadhav & et al, Towards enhanced security: An improved approach to phishing email detection, Journal of Electrical Systems, Vol. 20, No. 2, 2024, pp. 2763-2772.
14. Abdulla Al-Subaiey, Mohammed Al-Thani, Naser Abdullah Alam, Kaniz Fatema Antora, Amith Khandakar, SM Ashfaq Uz Zaman, Novel interpretable and robust web-based AI platform for phishing email detection, Computers and Electrical Engineering, Vol. 120, Part A, 2024, doi: 10.1016/j.compeleceng.2024.109625.
15. A. Enhancing, Arabic Phishing Email Detection: A Hybrid Machine Learning Based on Genetic Algorithm Feature Selection, International Journal of Advanced Computer Science & Applications, Vol. 15, No. 8, 2024, p. 312, doi: 10.14569/ijacsa.2024.0150832
16. Anirudh S, P Radha Nishant, Sanjay Baitha, K Dinesh Kumar, An Ensemble Classification Model for Phishing Mail Detection, Procedia Computer Science, Vol. 233, 2024, pp. 970-978, doi: doi.org/10.1016/j.procs.2024.03.286.

References

1. Most Common Types of Phishing Attacks in 2024. URL: https://www.upguard.com/blog/types-of-phishing-attacks (application date 2.09.2024)
2. Phishing Attacks: Statistics and Examples. URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing

(application date 2.09.2024)

3. Trends in the development of phishing and countering it. URL: https://my-itspecialist.com/trends-in-phishing-development-and-countermeasures (application date 3.09.2024)

4. Trends in Cyber Challenges and Solutions 2024. URL: https://www.h-x.technology/blog/trends-cyber-challenges-solutions-2024 (application date 4.09.2024)

5. Avoiding Social Engineering and Phishing Attacks. URL: https://www.penncommunitybank.com/wp-content/uploads/2021/06/Avoiding-Social-Engineering-and-Phishing-Attacks.pdf (application date 4.09.2024)

6. Understanding Social Engineering Tactics: 8 Attacks to Watch Out For. URL: https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for (application date 9.09.2024)

7. Phishing activity trends report. URL: https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf (application date 9.09.2024)

8. Francesco Greco, Giuseppe Desolda, Andrea Esposito, Alessandro Carelli. David versus Goliath: Can Machine Learning Detect LLM-Generated Text? A Case Study in the Detection of Phishing Emails, ITASEC: The Italian Conference on CyberSecurity, Italy, Vol. 3731, 2024.

9. P. R. Uyyala. Phishing email detection using CNN, Journal of Engineering and Technology Management, Vol. 72, 2024, pp. 1046-1051.

10. S. A.Nabi, G. Srija, G. Madhuri, M. R. Reddy, C. Jashuva, Phishing email detection using improved RCNN with multilevel. International Journal For advanced research in science & technology, Vol. 13, No. 7, 2023, pp. 63–69.

11. J.Keerthika, A. Adisvara, S. Akash, B. Jayanesh, T. Arul Prakash, E-mail spam detection and phishing link detection using machine learning, Advances in Computational Intelligence in Materials Science, 2023, pp. 47-53, doi: 10.53759/acims/978-9914-9946-9-8_9.

12. Jude Osamor et al, Real-Time Detection of Phishing Emails Using XG Boost Machine Learning Technique, International Conference on Information Technologies and Smart Systems, India, 2024.

13. G. B. Sambare, S. B. Galande, S. Kale, P. Nehete, V. Jadhav & et al, Towards enhanced security: An improved approach to phishing email detection, Journal of Electrical Systems, Vol. 20, No. 2, 2024, pp. 2763-2772.

14. Abdulla Al-Subaiey, Mohammed Al-Thani, Naser Abdullah Alam, Kaniz Fatema Antora, Amith Khandakar, SM Ashfaq Uz Zaman, Novel interpretable and robust web-based AI platform for phishing email detection, Computers and Electrical Engineering, Vol. 120, Part A, 2024, doi: 10.1016/j.compeleceng.2024.109625.

15. A. Enhancing, Arabic Phishing Email Detection: A Hybrid Machine Learning Based on Genetic Algorithm Feature Selection, International Journal of Advanced Computer Science & Applications, Vol. 15, No. 8, 2024, p. 312, doi: 10.14569/ijacsa.2024.0150832

16. Anirudh S, P Radha Nishant, Sanjay Baitha, K Dinesh Kumar, An Ensemble Classification Model for Phishing Mail Detection, Procedia Computer Science, Vol. 233, 2024, pp. 970-978, doi: doi.org/10.1016/j.procs.2024.03.286.