Цінність підходу полягає у скороченні часу між появою ознак атаки та рішенням щодо реагування. AI-модуль може об'єднати невдалу автентифікацію, нетиповий трафік, звернення до критичного сервера та зміну поведінки користувача в один інцидент із підвищеним пріоритетом. Водночас остаточне рішення має ухвалювати фахівець з урахуванням організаційного контексту. Основними ризиками впровадження AI є залежність від якості навчальних даних, хибнопозитивні або хибнонегативні спрацювання, складність пояснення рішень і вразливість моделей до маніпуляцій. Оскільки ISO/IEC 27005 розглядає управління ризиками як безперервний процес [4], AI-рішення мають супроводжуватися аудитом даних, перевіркою моделей, контролем доступу та журналюванням рекомендацій.

Отже, штучний інтелект є перспективним інструментом підтримки прийняття рішень у кібербезпеці, що підвищує швидкість аналізу, покращує пріоритезацію інцидентів і сприяє обґрунтованому реагуванню. Подальші дослідження доцільно спрямувати на пояснювані AI-моделі для SOC-середовищ, оцінювання довіри до автоматизованих рекомендацій і захист AI-модулів від цілеспрямованих атак.

1. Kaur R., Gabrijelcic D., Klobucar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023. Vol. 97. Article 101804.
2. Rjoub G. et al. A survey on explainable artificial intelligence for cybersecurity. IEEE Transactions on Network and Service Management. 2023. Vol. 20(4). P. 5115-5140.
3. Capuano N., Fenza G., Loia V., Stanzione C. Explainable artificial intelligence in cybersecurity: A survey. IEEE Access. 2022. Vol. 10. P. 93575-93600.
4. Sarker I.H. et al. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data. 2020. Vol. 7. Article 41.

Analysis of modern methods for detecting phishing domains and links

UDK 004.056.5:004.738.5

Ivan Azarov[1], Anna Korchenko[2],
Illia Azarov[3], Kyrylo Davydenko[4]

State University of Communication and Informational Technologies,
[1]azarovphone@gmail.com,
NTU Dnipro Polytechnic, [2]annakor@ukr.net, [4]kirilldavy@gmail.com,
Kyiv Aviation Institute, [3]azarovforce@gmail.com

Phishing remains one of the most common cyberattack vectors, utilizing social engineering and technical masking techniques to steal confidential data.

With the emergence of automated tools, attackers have gained the ability to mass-generate deceptive URLs and clone legitimate web resources, which reduces the effectiveness of traditional security measures.

The use of comprehensive approaches to analyzing domains and links is critical for countering phishing attacks, particularly zero-day attacks [1].

The main objective of this study is to analyze the methods and criteria for detecting phishing domains and URLs, as well as to evaluate their effectiveness, speed, and practical feasibility in modern cybersecurity systems.

The process of identifying phishing resources involves checking various levels: from analyzing the URL structure to examining the webpage content. For a comprehensive review, 10 fundamental detection methods were identified.

1. Use of blacklists. The method is based on comparing the requested URL with global databases of known malicious links (e.g., Google Safe Browsing, PhishTank). If the domain is found in the database, access to it is automatically blocked. This is the oldest and most basic approach to filtering internet traffic.

2. Use of trusted site lists. The method relies on utilizing global rankings of the world's most popular and trusted domains (e.g., the top 1 million domain lists by Tranco or Cisco Umbrella). Resources included in this list are considered safe by default and are bypassed by the system without deep inspection. This approach works as a fast pre-filter to separate the bulk of legitimate traffic [2].

3. Lexical analysis of URLs. The method examines the structure of the link itself: URL length, presence of special characters, use of an IP address instead of a domain, and typosquatting. It operates at the text level, detecting statistical anomalies that are atypical for legitimate sites.

4. Analysis of DNS and WHOIS records. The method evaluates a domain's reputation based on data regarding its registration, age, time-to-live (TTL), and history of IP address changes. Phishing domains typically have an age of a few days and are registered in cheap or free zones.

5. Hosting and network reputation analysis. Verifies whether the domain's IP address belongs to a specific Autonomous System (ASN) and evaluates the hosting provider's reputation. Attackers often choose specific, abuse-tolerant data centers or networks compromised by botnets.

6. Analysis of SSL/TLS certificates. Checks the presence, type, and issuer of the cryptographic certificate. Today, domain name mismatches within the certificate or the mass use of free solutions (Let's Encrypt) are analyzed, since the presence of basic HTTPS is no longer a guarantee of security.

7. Analysis of HTML content and page structure. The method involves downloading the page code to search for hidden iframes, suspicious login collection forms, and external link mismatches (when a form sends data to a third-party domain). The method records actual malicious activity on the site.

8. Visual analysis of the page. Takes a screenshot of the web page and compares its graphic elements (logos, structure, color scheme) with reference samples of well-known brands. It uses neural networks to evaluate the percentage of visual similarity [3].

9. Analysis of redirection chains. Tracks all HTTP redirects from the initial link to the final page. Phishers often use multiple redirects through shortening services to hide the final malicious domain from security filters [4].

10. Search indexing analysis. Checks whether the domain is present in the organic search results of search engines (Google, Bing) and what its ranking is. Most phishing sites do not have time to get indexed or are quickly blocked by search algorithms [5].

Based on the comprehensive analysis conducted, the following conclusions can be drawn: there is no single universal method for detecting phishing. The simplest and fastest methods (blacklists, trusted lists of the top million domains) are excellent primary filters due to their ease of implementation, but their standalone detection effectiveness is insufficient against modern zero-day threats. Methods of visual analysis and HTML content inspection demonstrate the highest accuracy, but they are too slow for stream processing. Therefore, an effective modern phishing detection system must be combined and include the following parameters: fast lists and lexical analysis filter out mass traffic, after which resource-intensive content or visual analysis using artificial intelligence is applied to suspicious links.

1. Li, W., Manickam, S., Chong, Y. W., Leng, W., & Nanda, P. (2024). A state-of-the-art review on phishing website detection techniques. IEEE Access, 12, 187976-188012.
2. Azeez, N. A., Misra, S., Margaret, I. A., Fernandez-Sanz, L., & Abdulhamid, S. I. M. (2021). Adopting automated whitelist approach for detecting phishing attacks. Computers & Security, 108, 102328.
3. Kustiawan, Y. A., & Ghauth, K. I. (2025). Feature Engineering for Phishing Website Detection Using Machine Learning: A Systematic Review. *IEEE Access*, *13*, 192080-192104.
4. Lamina, O. A., Ayuba, W. A., Adebiyi, O. E., Michael, G. E., Samuel, O. O. D., & Samuel, K. O. (2024). AI-powered phishing detection and prevention. *Path of Science*, *10*(12), 4001-4010.
5. Alazaidah, R., BaniSalman, M., Alqawasmi, K. E., Abu Zaid, A., Hazaimeh, Y., Alshraiedeh, F. S., & Qumsiyeh, E. (2026). Identifying key features for phishing website detection through feature selection techniques. Frontiers in Computer Science, 7, 1687867.

Симетричний ієрархічний криптоалгоритм на основі Китайської теореми про залишки

УДК 004.056.55

Ігор Якименко[1], Степан Івасьєв[2]

Західноукраїнський національний університет,
[1] jiz@wunu.edu.ua, [2]isv@wunu.edu.ua

Сучасний розвиток інформаційно-комунікаційних технологій супроводжується постійним зростанням обсягів передавання даних та підвищенням вимог до їх криптографічного захисту. Особливо актуальними є задачі забезпечення конфіденційності інформації у багаторівневих інформаційних системах, де необхідно поєднувати високу криптостійкість із швидкодією процесів шифрування та дешифрування. У зв'язку з цим значний інтерес становлять криптографічні методи, побудовані на основі систем залишкових класів (СЗК) [1, 2] та Китайської теореми про залишки (КТЗ) [3].

У роботі [4] досліджено теоретичні основи симетричних криптоалгоритмів у СЗК та показано, що криптостійкість таких методів визначається кількістю модулів і їх розрядністю. Подальший розвиток даного напряму пов'язаний із