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

використанням ієрархічних структур СЗК. У праці [5] запропоновано симетричний криптоалгоритм на основі ієрархічної СЗК, який забезпечує поетапне зменшення розрядності модулів та операндів на кожному рівні шифрування і характеризується комбінаторною криптостійкістю до криптоаналітичних атак.

Незважаючи на існуючі дослідження, питання побудови ефективних симетричних ієрархічних криптосистем на основі Китайської теореми про залишки залишаються актуальними, зокрема в частині оптимізації швидкодії розшифрування та забезпечення багаторівневого захисту інформації.

Метою роботи є розроблення симетричного ієрархічного криптоалгоритму на основі Китайської теореми про залишки, який забезпечує багаторівневе шифрування інформації та підвищує ефективність процесу розшифрування за рахунок використання модульного представлення даних.

В симетричній ієрархічній криптосистемі на основі КТЗ обом абонентам повинні бути відомі модулі p_{ji} – ключі, де j – ієрархічний рівень, i – кількість модулів. Відкрите повідомлення S у цифровій формі на першому ієрархічному рівні розбивається на блоки S_{1i}, для кожного з яких виконується умова $S_{1i} < p_{1i}$, де p_{1i} – модулі (ключі) першого рівня. Шифрування відбувається згідно КТЗ:

$$S_1 = \left(\sum_{i=1}^{k} \quad S_{1i} M_{1i} m_{1i}\right) P_1 \,, \tag{1}$$

де $P_1 = \prod_{i=1}^{k} \quad p_{1i}$, $M_{1i} = \frac{P_1}{p_{1i}}$, m_{1i} шукається з виразу $m_{1i} = M_{1i}^{-1} p_{1i} \; = 1$, k – кількість модулів, S_1 – шифротекст першого рівня.

Після чого S_1 розбивається на блоки S_{2i} , для яких виконується умова $S_{2i} < p_{2i}$ і передається на другий ієрархічний рівень і ширується згідно співвідношення:

$$S_2 = \left(\sum_{i=1}^{k} \quad S_{2i} M_{2i} m_{2i}\right) P_2 \,, \tag{2}$$

де $P_2 = \prod_{i=1}^{k} \quad p_{2i}$, $M_{2i} = \frac{P_2}{p_{2i}}$, m_{2i} шукається з виразу $m_{2i} = M_{2i}^{-1} p_{2i} \; = 1$, k – кількість модулів, S_2 – шифротекст другого рівня.

Відповідно на j – тому ієрархічномі рівні отримується шифротекст S_j згідно формули:

$$S_j = \left(\sum_{i=1}^{k} \quad S_{ji} M_{ji} m_{ji}\right) P_j \,, \tag{3}$$

де $P_j = \prod_{i=1}^{k} \quad p_{ji}$, $M_{ji} = \frac{P_j}{p_{ji}}$, m_{ji} шукається з виразу $m_{ji} = M_{ji}^{-1} p_{ji} \; = 1$, k – кількість модулів, S_j – шифротекст j – того ієрархічного рівня передається по відкритому каналі зв'язку до отримувача.

Дешифрування відбувається у зворотньому порядку з j – того ієрархічного рівня до першого згідно формули:

$$S_{ji} = S_j mod p_{ji} \tag{4}$$

На першому рівні отримуємо блоки S_{1i}, які в результаті конкатенації відновлюють вхідне повідомлення S. Запропонований симетричний метод шифрування доцільно використовувати, коли потрібне швидке дешифрування, оскільки на цьому етапі необхідно виконання тільки операції пошуку залишків.

У роботі запропоновано симетричний ієрархічний криптоалгоритм на основі КТЗ, який реалізує багаторівневе шифрування інформації шляхом

послідовного перетворення даних у системі взаємно простих модулів. Особливістю методу є використання ієрархічної структури ключів, що дозволяє організувати багаторівневий захист інформації та підвищити гнучкість криптографічної системи.

Використання модульного представлення даних сприяє зменшенню обчислювальної складності окремих операцій та створює передумови для паралельної обробки інформації.

Дослідження показали, що запропонований метод доцільно використовувати в інформаційних системах, де важливими є швидке дешифрування даних, багаторівневий доступ та підвищені вимоги до захисту інформації.

1. Omondi A., Premkumar B. Residue number systems: theory and implementation. London: Imperial College Press, 2007. 296 p.
2. Singh N. An overview of Residue Number System. Devices, Circuits & Communication: Proceedings of the National Seminar. 2008, pp. 132-135.
3. Verma S., Garg D. Improvement in rebalanced CRT RSA. *International Arab Journal of Information Technology*. Vol.12, No. 6, 2015, pp.524-532.
4. M. M. Kasianchuk, I. Z. Yakymenko, Ya. M. Nykolaychuk Symmetric Cryptoalgorithms in the Residue Number System. Cybernetics and Systems Analysis, 2021, Vol 57, Issue 2, p.184-189. https://doi.org/10.1007/s10559-021-00358-6
5. Yakymenko I., Kasianchuk M., Martyniuk O., Martyniuk S. A Symmetric Cryptoalgorithm Based on a Hierarchical Residue Number System. International Journal of Computing, 2025. 24(1), pp. 92-101. https://doi.org/10.47839/ijc.24.1.3880

Оцінка ефективності Counter-OSINT стратегій за допомогою теорії інформації

УДК 004.056.5:519.72

Валерія Івкова[1], Іван Опірський[2]

Національний університет «Львівська політехніка» ,
[1]valeriia.s.ivkova@lpnu.ua, [2]ivan.r.opirskyi@lpnu.ua

Стрімка діджиталізація та гібридні загрози дозволяють ворожим аналітикам реконструювати детальні цифрові профілі через OSINT-технології з мінімальними витратами ресурсів, що зумовлює перехід від пасивної цифрової гігієни до проактивних Counter-OSINT стратегій.

З позиції теорії інформації, ефективність таких стратегій доцільно вимірювати обсягом когнітивних та часових ресурсів, необхідних атакуючій стороні для відновлення цілісного "корисного сигналу" цифрової ідентичності з наявних даних. У цьому контексті виділяють два концептуальні підходи: обфускацію та компартменталізацію.

Метод обфускації фокусується на зниженні співвідношення сигнал/шум шляхом генерації надлишкової хибної інформації. Проте сучасні автоматизовані OSINT-засоби та алгоритми машинного навчання здатні