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

ефективно фільтрувати цей "шум", виокремлюючи справжні «точки дотику», що дозволяє порівняно легко відновити граф ідентичності [1].

Метод компартменталізації - заснований на військовій моделі «need-to-know», передбачає логічну та технічну ізоляцію цифрових ідентичностей на рівнях операційної системи, браузера та мережевого трафіку. Цей підхід фізично розриває зв'язки між фрагментами даних, повністю фрагментуючи граф ідентичності та позбавляючи аналітика "точок дотику" [2 с.73].

З позиції теорії інформації, цифрову ідентичність об’єкта можна представити як систему станів X. Разом із тим ефективність протидії OSINT оцінюється через збільшення невизначеності (ентропії) для аналітика.

Ефективність обфускації базується на штучному підвищенні ентропії системи шляхом внесення надлишкового шуму N. Проте зловмисник може використовувати алгоритми фільтрації для мінімізації відстані Кульбака-Лейблера [3] (D_{KL}), яка вимірює розбіжність між розподілом ймовірностей зашумлених даних $P(x)$ та реальним профілем $Q(x)$:

$$D_{KL}(P\|Q) = \sum_{x\epsilon X} P(x)\ log\ log\ \frac{P(x)}{Q(x)} \tag{1}$$

При використанні автоматизованих OSINT-засобів значення D_{KL} стрімко зменшується, що вказує на низьку стійкість обфускації до машинного аналізу.

На відміну від обфускації, компартменталізація спрямована на мінімізацію взаємної інформації $I(X;Y)$ між різними сегментами ідентичності X та Y:

$$I(X;Y) = H(X) + H(Y) - H(X,Y) \tag{2}$$

де $H(X,Y)$ — спільна ентропія сегментів. Стратегія вважається успішною, якщо $I(X;Y) \to 0$, що означає повну відсутність кореляції між фрагментами даних. Це фізично унеможливлює автоматизоване поєднання профілю через відсутність точок дотику.

Ефективність стратегії E визначається як функція від складності відновлення сигналу C:

Для обфускації:

$$cobf \approx log\left(\frac{S}{N}\right) \tag{3}$$

де S/N — співвідношення сигнал/шум. Витрати атакуючої сторони зростають лише лінійно.

Для компартменталізації:

$$C_{comp} = \sum_{i=1}^{n} Ti \tag{4}$$

де Ti — час на окреме ручне дослідження кожного ізольованого сегмента n.

Математичне моделювання доводить, що компартменталізація забезпечує експоненціальне зростання витрат зловмисника, оскільки розриває логічні

зв'язки в графі ідентичності, тоді як обфускація лише тимчасово ускладнює обробку даних.

Таким чином, головна перевага компартменталізації над обфускацією полягає в тому, що вона ускладнює можливість автоматизованої кореляції даних, що змушує атакуючу сторону переходити від швидкого збору інформації до складного, ресурсомісткого та часто безрезультатного ручного інтелектуального розслідування.

Проте, поряд із високою ефективністю, метод компартменталізації накладає значні обмеження на користувача та потребує підвищених апаратних ресурсів для підтримки декількох ізольованих середовищ. Це створює поріг входження для пересічного користувача, проте є виправданим компромісом у контексті експоненціального зростання витрат атакуючої сторони

1. Cheng, H., Qiang, C., Cong, L., Xiao, J., Liu, S., Zhou, X., Wang, H., Ruan, M., & Lv, C. (2025). A Novel Data Obfuscation Framework Integrating Probability Density and Information Entropy for Privacy Preservation. *Applied Sciences*, *15*(3), 1261. https://doi.org/10.3390/app15031261
2. Івкова В.С., & Опірський І.Р., (2025). Дослідження можливості інтеграції методу компартменталізації у захист інформації у відкритих джерелах. *Computer systems and network*, *7*(2), 71–83. https://doi.org/10.23939/csn2025.02.071
3. Lopes, A. O., & Mengue, J. K. (2022). On information gain, Kullback-Leibler divergence, entropy production and the involution kernel. *Discrete & Continuous Dynamical Systems*, 0. https://doi.org/10.3934/dcds.2022026

Сучасний стан кібербезпеки в Україні

УДК 004.056.53

Кардашук Володимир[1]

Східноукраїнський національний університет, [1]kardashuk1@snu.edu.ua

Стрімкий розвиток інформаційних технологій суттєво випереджає створення надійних умов захисту цифрового кіберпростору. Для сучасного економічного розвитку критичним є забезпечення особистої безпеки, бізнесу та держави. Актуальним завданням сьогодення є створення комплексу заходів спрямованих на захист інформаційних ресурсів від кібератак, небажаного доступу, інших дій на модифікацію або знищення важливих даних. Сучасне інформаційне оточення швидко змінюється, що вимагає динамічно реагувати на загрози, адаптуватись до викликів та кібернетичних атак. Все більша кількість загроз, методів та стратегій використовує вразливості кіберзахисту.

Аналіз сучасного стану кібербезпеки в Україні показав недостатню координацію між суб'єктами кібербезпеки, що ускладнює координацію на кіберзагрози [1].

В останні роки підмічена тенденція еволюціонування загроз з незмінними мотивами фінансової вимоги [2].