перетворення у машинні інструкції та провести статичний аналіз без необхідності роботи з динамічно згенерованим кодом.

Висновки. У ході роботи було проаналізовано і розроблено методи виявлення сучасного шкідливого програмного забезпечення. Знайдено недоліки в існуючих рішеннях аналізу шкідливого ПЗ та розроблено власний метод виявлення шкідливого програмного забезпечення, спрямований на виявлення ШПЗ, яке користується компіляцією під час виконання для приховування свого шкідливого тіла. Розроблений код може бути використаний як основа для майбутніх інструментів виявлення ШПЗ, або також інструмент може використовуватися як самостійний інструмент аналізу.

ПЕРЕЛІК ПОСИЛАНЬ

1. *ptrace(2) - Linux manual page*. (б. д.). Michael Kerrisk - man7.org. https://man7.org/linux/man-pages/man2/ptrace.2.html

2. *The LLVM Compiler Infrastructure Project. (б. д.). The LLVM Compiler Infrastructure Project. https://llvm.org/*

УДК 004.056.5

Демченко О.Ф.,[1] Літвінова О.В.[2], Євсеєв С.П.[3]

ОЦІНКА КРИПТОСТІЙКОСТІ МЕХАНІЗМІВ ШИФРУВАННЯ НА ОСНОВІ ЕНТРОПІЙНОГО МЕТОДУ

Вступ. Розвиток сучасних технологій, у першу чергу квантових комп'ютерів, вимагає більш жорстких вимог до криптосистем у постквантовий криптоперіод. Поява повномасштабного квантового комп'ютера ставить під сумнів можливість забезпечити послуги безпеки методами симетричної та несиметричної криптографії. Злам симетричних криптосистем спроможний за рахунок використання квантових ресурсів на основі алгоритму Гровера, а несиметричних криптосистем за рахунок алгоритму Шора. У таких умовах швидка оцінка стійкості запропонованих програмних (програмно-апаратних) застосунків на основі симетричної та несиметричної криптографії стає актуальним питанням. Крім цього, порівняльний аналіз різних реалізацій криптоалгоритмів різними виробниками також можливий за рахунок запропонованого рішення на основі ентропійного методу оцінки випадковості криптограми.

Мета роботи. Дослідження методів оцінки криптостійкості

[1] учень 10-А класу комунального закладу "Харківський ліцей № 124 Харківської міської ради"

[2] учитель інформатики комунального закладу "Харківський ліцей № 124 Харківської міської ради", вища категорія, старший учитель

[3] д.т.н., проф., завідувач кафедри кібербезпеки НТУ «ХПІ»

сучасних алгоритмів шифрування шляхом обчислення інформаційної ентропії та порівняльний аналіз їх ефективності при обробці різних типів даних.

Методи та результати дослідження. В основі дослідження лежить математичний апарат теорії інформації К. Шеннона. Для оцінки стійкості використовується формула обчислення інформаційної ентропії:

$$H(X) = -sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$$

де $p(x_i)$ — ймовірність появи і-го символу в алфавіті повідомлення. Для ідеального шифру значення ентропії має наближатися до максимуму, що свідчить про рівномірний розподіл символів у криптограмі. На рис. 1 наведений алгоритм розгляду ентропійного методу оцінки стійкості симетричних та несиметричних криптосистем. Відомо, що максимально можливий криптографічний захист дає так званий "Ідеальний шифр" за Шенноном, який у результаті шифрування дає випадкове число [1].

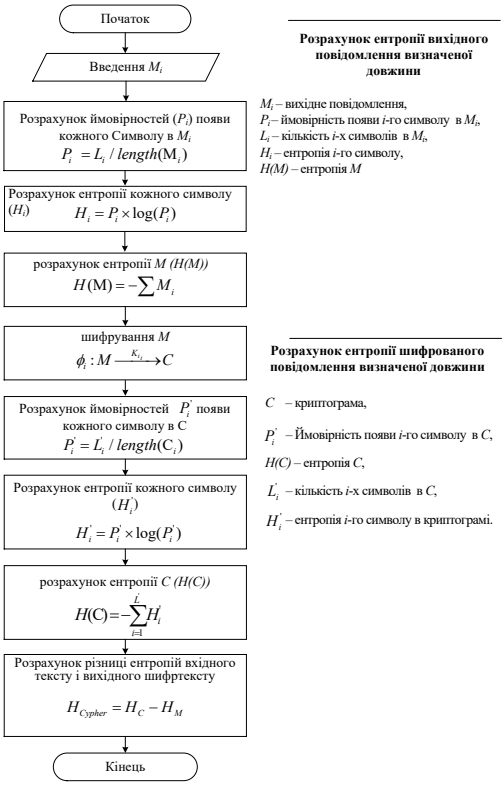

Рисунок 1. Алгоритм тестування криптосистеми на стійкість на основі ентропійного методу оцінки випадковості

Такий файл характеризується максимальною ентропією, яка для бінарного випадку дорівнює одиниці. Вважатимемо, що шифрування за допомогою такого шифру забезпечує максимальний рівень криптографічного захисту, прийнятий за 1, тобто ймовірність захисту також дорівнює одиниці. Очевидно, що неідеальні шифри не забезпечують такого рівня надійності. На рис. 2 наведено результати дослідження усередненої ентропії криптограм різних БСШ для осмисленого відкритого тексту довжиною $M = 10^8$біт з інтервалом $N = 5 \times 10^6$біт

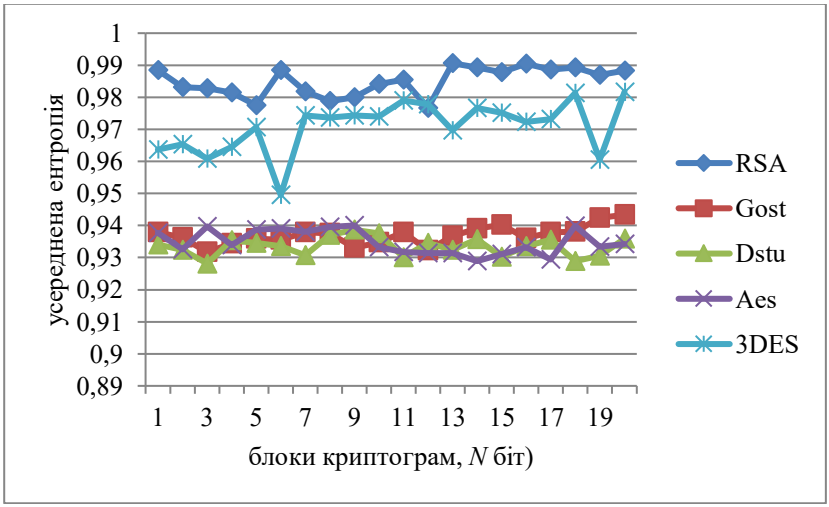

Рисунок 2. Результати досліджень усередненої ентропії блоків криптограм

Аналіз рис. 2 фактично підтверджує доцільність застосування експрес-методу для вибору програмного забезпечення механізмів безпеки на основі криптоалгоритмів. Отримані результати свідчать, що простий експрес-метод, заснований на ентропійному оцінюванні випадковості криптограми, дозволяє оперативно визначати якість використовуваних шифрів без залучення експертів і значних економічних, обчислювальних та трудових ресурсів. [5]

Висновки. Проведене дослідження підтвердило, що ентропійний метод є ефективним інструментом для кількісної оцінки захищеності інформаційних систем. Запропоновані модифікації алгоритмів дозволяють підвищити криптостійкість до рівня, при якому статистичні методи дешифрування стають економічно та технічно недоцільними. Подальші дослідження будуть спрямовані на оптимізацію швидкодії ентропійних алгоритмів для роботи в системах реального часу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., & Milov, O. (Eds.). (2021). *Synergy of building cybersecurity systems*. PC TECHNOLOGY CENTER.
2. Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson. https://www.pearsonhighered.com/program/Stallings-Cryptography-and-Network-Security-Principles-and-Practice-7th-Edition/PGM334401.htm
3. Python Software Foundation. (n.d.). *Secrets — Generate secure random numbers for managing secrets*. https://docs.python.org/3/library/secrets.html
4. Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C*. John Wiley & Sons.
5. Євсеєв, С. П., Король, О. Г., Корольов, Р. В., & Піх, Ю. Р. (2018). Статистичний метод оцінки стійкості на основі ентропійного методу. Інформаційна безпека, (3), 5–12. http://repository.hneu.edu.ua/bitstream/123456789/20201/1/Інформаційна%20безпека%202018%20(3).pdf

УДК 004.9

Палєєв М.А.[1], Палєєва К.М. [2]

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПРОФЕСІЙНОМУ ВИБОРІ В ТЕХНІЧНІЙ СФЕРІ (НА ПРИКЛАДІ НАФТОГАЗОВОЇ ГАЛУЗІ)

На сьогодні у молоді Україні серед майбутніх професій стабільно популярними залишаються гуманітарні спеціальності, такі як менеджмент, філологія, психологія, право, маркетинг тощо. У той саме час більшість інженерних спеціальностей, зокрема в галузі енергетики, механіки, будівництва та ін., залишаються поза увагою абітурієнтів. Хоча держава економічно і законодавчо заохочує молодь до вступу на критично важливі напрямки (додаткові бали при вступі, нижча вартість контракту, вищі стипендії, тощо), однак популярність цих галузей не в останню чергу залежить від методів проведення профорієнтації та презентації спеціальностей майбутнім абітурієнтам, наприклад, шляхом залучення сучасних технологій [1]. У даному дослідженні на прикладі нафтогазової галузі розглянуто роль цифрових технологій у професійному виборі молоді в технічній сфері.

Нафтогазова галузь є дуже важливою для економіки нашої країни, оскільки вона забезпечує енергоресурсами промислові підприємства і населення, а також є одним з основних платників податків та інвесторів в економіку країни. Однак, не дивлячись на доволі високу заробітну

[1] Учень Харківської гімназії І-ІІІ ступеня № 77
[2] Старший викладач кафедри НІіТ, ХНУМГ ім. О. М. Бекетова