УДК 004.056.5:004.8
О. Цвірла; І. Мудрий; Н. Луцик, доктор філософії, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ОЦІНЮВАННЯ КРИПТОГРАФІЧНОЇ ЯКОСТІ ХЕШ-СТРІЧОК У ІНФОРМАЦІЙНИХ СИСТЕМАХ

UDC 004.056.5:004.8
O. Tsvirla; I. Mudryi; N. Lutsyk, PhD., Assoc. Prof.

INTELLIGENT METHODS FOR ASSESSING THE CRYPTOGRAPHIC QUALITY OF HASH STRINGS IN INFORMATION SYSTEMS

Сучасні інформаційні системи широко використовують хеш-функції для забезпечення автентифікації, контролю цілісності та захисту проміжних даних у комунікаційних та обчислювальних процесах. Поширення застарілих або криптографічно слабких алгоритмів створює значні ризики для стабільності комп'ютерно-інформаційних технологій і систем зв'язку, особливо в умовах стрімкого розвитку апаратного прискорення та зростання обчислювальних потужностей [1–2].

Проблемним аспектом є відсутність інструментів, здатних оцінювати якість хеш-функцій не за формальними ознаками алгоритму, а за реальними структурними характеристиками сформованих хеш-рядків. Для підвищення рівня криптографічної стійкості інформаційних інфраструктур актуальним стає застосування методів інтелектуального аналізу, що дозволяють визначати потенційний рівень небезпеки хеш-значень на основі їх внутрішніх властивостей.

Перспективним напрямом є використання математичних моделей, зорієнтованих на аналіз ентропійних характеристик, алфавітних розподілів, довжини, структурної варіативності та поведінкових патернів хеш-стрічок. Таке багатовимірне представлення ознак дає змогу розмежовувати стійкі та вразливі хеш-функції без застосування криптоаналітичних атак або перебору.

Використання інтелектуальних алгоритмів машинного навчання забезпечує автоматизоване оцінювання криптографічного ризику у великих масивах даних у режимі реального часу. Інтеграція багатопотокових механізмів обробки дозволяє впроваджувати такі підходи в масштабовані інформаційні системи, телекомунікаційні мережі та інші високонавантажені технологічні середовища, де критичною є безперервність і надійність інформаційних потоків.

Важливою складовою інтелектуального аналізу є здатність моделі адаптуватися до нових алгоритмів хешування та змінених параметрів існуючих криптографічних стандартів. Використання адаптивних підходів дозволяє підтримувати актуальність оцінювання навіть у разі появи модифікованих схем хешування або нових форматів даних, типових для корпоративних екосистем та хмарних інфраструктур.

Крім того, застосування інтелектуальних механізмів пріоритизації ризиків забезпечує можливість автоматичного виділення критично небезпечних хеш-значень, що потребують негайної уваги адміністратора. Формування рейтингу криптографічної небезпеки підвищує ефективність прийняття рішень та сприяє оптимізації політик безпеки. Це створює передумови для побудови проактивних систем захисту, здатних адаптуватися до нових векторів атак і забезпечувати стабільність інформаційних сервісів.

Застосування інтелектуальних криптоаналітичних методів сприяє зміцненню стійкості каналів зв'язку, зменшенню ризику несанкціонованого доступу та підвищенню загального рівня безпеки сучасних комп'ютерно-інформаційних технологій. Це формує основу для створення адаптивних систем захисту, здатних реагувати на нові типи загроз та забезпечувати належний рівень криптографічної надійності у динамічних інфраструктурах.

Література

1. Stallings W. *Cryptography and Network Security.* Pearson, 2023. С. 145–210.
2. Aghaei A., Homayoun H., Sasan A. 2020. *Hash Function Security Evaluation via Machine Learning-Based Structural Analysis.* ACM, С. 1–10.