2019.- № 2. С.115-122. URL http://nbuv.gov.ua/UJRN/Infpr 2019 (дата звернення: 10.02.2024).

ЛУНГОЛ Ольга – *доцентка кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ, кандидатка педагогічних наук, доцент*

УДОСКОНАЛЕННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ПРОТИДІЇ ЗЛОЧИННОСТІ

В умовах стрімкого розвитку інформаційних технологій та зростання кількості кіберзагроз, забезпечення захисту інформації стає пріоритетним завданням для правоохоронних органів. Криптографічні алгоритми відіграють ключову роль у захисті даних, які використовуються для протидії злочинності, особливо в контексті організованої злочинності та кіберзлочинів. Постійне удосконалення цих алгоритмів є необхідністю для збереження конфіденційності, цілісності та доступності інформації. Зокрема, новітні загрози, пов'язані з розвитком квантових обчислень, вимагають перегляду існуючих методів шифрування та розробки пост-квантових криптографічних алгоритмів, які зможуть забезпечити належний рівень захисту навіть в епоху квантових обчислень.

З розвитком квантових обчислень традиційні криптографічні методи, такі як RSA (Rivest–Shamir–Adleman) та ECC (Elliptic Curve Cryptography) [1], стають вразливими до атак квантових комп'ютерів. У зв'язку з цим постає нагальна потреба у розробці нових криптографічних алгоритмів, здатних забезпечити надійний захист інформації в епоху квантових обчислень. Такі алгоритми отримали назву пост-квантових криптографічних алгоритмів. Більшість традиційних криптографічних алгоритмів базується на складності задач розкладу великих чисел на прості множники або обчисленні дискретного логарифму. Квантові комп'ютери в свою чергу, використовуючи алгоритм Шора, можуть ефективно вирішувати ці задачі, що робить традиційні методи вразливими. Квантові комп'ютери можуть швидко вирішувати задачі факторизації великих чисел, які є основою для безпеки традиційних криптографічних методів, таких як RSA. Алгоритм Шора здатний розкласти число на прості множники за поліноміальний час, що робить його надзвичайно ефективним у порівнянні з класичними алгоритмами, які працюють за експоненційний час. Це означає, що криптографічні схеми, які залежать від складності факторизації, можуть бути зламані за значно коротший час, ставлячи під загрозу безпеку даних у разі появи достатньо потужних квантових комп'ютерів.

Існує кілька основних напрямків досліджень у галузі пост-квантової криптографії, серед яких можна виділити криптографію на решітках (або криптографію на алгебраїчних решітках, криптографію на основі решіток), багатозначну криптографію, кодову криптографію та хеш-базовану криптографію [2 – 5].

Криптографія на решітках вважається однією з найперспективніших галузей пост-квантової криптографії. Вона базується на складності задач, пов'язаних з векторними просторами та ґратками (решітками). Ці задачі є надзвичайно складними для класичних комп'ютерів і, можливо, залишатимуться складними навіть для квантових комп'ютерів, що робить криптографію на решітках особливо перспективною для захисту інформації в епоху квантових обчислень. NTRUEncrypt, LWE (Learning With Errors) та їх варіанти є стійкими до атак квантових комп'ютерів. Вони мають високий рівень безпеки та ефективності, що робить їх перспективними для широкого застосування. Проте можна виділити і недоліки криптографії на решітках – великі розміри ключів та повідомлень, а також значні обчислювальні витрати, що можуть обмежити їхнє використання в деяких практичних сценаріях.

Багатозначна криптографія базується на складності розв'язання багатозначних рівнянь, але має недоліки у складності реалізації та певні обмеження в продуктивності, що потребує подальших досліджень та оптимізації. Кодова криптографія використовує складність задач декодування випадкових лінійних кодів. Вона має високий рівень стійкості до квантових атак і може бути ефективно реалізована для різних застосувань. Хеш-базована криптографія використовує односторонні хеш-функції для створення стійких криптографічних алгоритмів. Одним з прикладів є схема підпису Лампорт [5].

У контексті загрози, яку представляють квантові комп'ютери для сучасних криптографічних методів, пост-квантова криптографія стає критично важливим напрямом досліджень та розробок. Незважаючи на певні недоліки та виклики, такі як великі розміри ключів та обчислювальні витрати, які супроводжують впровадження пост-квантових алгоритмів, ці технології мають значний потенціал для забезпечення безпеки інформації в епоху квантових обчислень. У зв'язку з цим, подальші дослідження та оптимізація вище зазначених алгоритмів є вкрай важливими.

Пост-квантова криптографія здатна забезпечити захист критичної інформації в різних сферах, включаючи правоохоронну галузь, державне управління, фінанси, охорону здоров'я тощо. Завдяки високій стійкості до квантових атак, криптографія на решітках, кодова та хеш-базована криптографія можуть стати основою для розробки нових стандартів безпеки, які будуть здатні протистояти загрозам майбутнього.

Таким чином, впровадження пост-квантових криптографічних алгоритмів стає не лише технологічною вимогою, а й необхідною складовою ефективної протидії злочинності, зокрема організованим злочинним групам і кіберзлочинцям, які використовують новітні інформаційні технології для атак на державні та приватні інформаційні ресурси. Для правоохоронних органів, які

ведуть боротьбу зі злочинністю, пост-квантова криптографія є ключовим інструментом захисту даних, що стосується оперативної інформації, розслідувань та конфіденційних відомостей. Ефективне використання цих алгоритмів дозволить мінімізувати ризики витоку або компрометації критичної інформації, посилюючи інформаційно-аналітичну діяльність правоохоронних структур. Удосконалення криптографічних засобів стане важливим фактором у забезпеченні безпеки державних систем, які протистоять сучасним викликам цифрового світу та сприяють побудові стійкої інформаційної інфраструктури.

Список використаних джерел:

1. Лунгол О.М. Оцінка застосування криптографічних алгоритмів в системах автентифікації на основі біометричних даних. Наука і техніка сьогодні. № 8 (36), 2024. С. 1089 – 1102. DOI: https://doi.org/10.52058/2786-6025-2024-8(36)-1089-1102

2. Пащак С.А. Квантові і постквантові методи та засоби захисту інформації : кваліф. робота на здобуття освіт. Ступ. магістр за спец. «125 – кібербезпека» / С.А. Пащак. Тернопіль: ТНТУ, 2023. 109 с.

3. Petrenko O., Sievierinov O., Fiediushyn O,. Zubrych A., Shcherbina D. Analysis of ways to increase stability of cryptographic algorithms on algebraic lattices against time attacks. Radiotekhnika. № 4(207). Pp. 59–65. https://doi.org/10.30837/rt.2021.4.207.05

4. Нікітченко Б.Ю. Дослідження застосування методів пост-квантової криптографії для розподілених систем авторизації. URL: http://surl.li/buobes (Дата звернення 25.08.2024).

5. Горбенко І. Д., Халімов Г.З. Порівняльний аналіз одноразових підписів на базі геш-функцій. Всеукраїнський міжвідомчий науково-технічний збірник «Радіотехніка». Вип. 203. 2020. С. 5 – 18.

МОВЧАН Анатолій – *професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, доктор юридичних наук, професор*

ХАРАКТЕРИСТИКА СУЧАСНОЇ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ ЗА РЕЗУЛЬТАТАМИ ОПИТУВАННЯ SOCTA

Важливе значення у протидії організованій злочинності посідає використання методології SOCTA для визначення пріоритетів боротьби з організованою злочинністю. Зокрема, аналіз, представлений в останньому опитуванні SOCTA-2021, характеризує ключові ознаки сучасної організованої злочинності, такі як широке використання корупції, залучення легальних бізнес-структур для всіх видів злочинної діяльності, існування паралельної