УДК 681.3.07 (3.06) **DOI:10.30837/rt.2025.1.220.04**

Д.М. МОРГУЛЬ, О.П. НАРЄЖНІЙ, канд. техн. наук, Т.О. ГРІНЕНКО, канд. техн. наук

КЛАСИФІКАЦІЯ АТАК ТА ВИМОГИ КІБЕРБЕЗПЕКИ ДО ВЕБ-РЕСУРСУ QRNG

Вступ

Квантові генератори випадкових чисел (Quantum Random Number Generator, QRNG) є ключовими компонентами сучасних криптографічних систем, які забезпечують генерацію непередбачуваних чисел на основі квантових ефектів. Це дозволяє уникнути обмежень традиційних псевдовипадкових генераторів (Pseudo Random Number Generator, PRNG), що можуть бути вразливими до прогнозування або відтворення. QRNG використовують фундаментальні принципи квантової механіки, зокрема властивості фотонів або електронів, для створення справжньої випадковості. На відміну від PRNG, які базуються на алгоритмічному підході, QRNG є стійкими до будь-яких спроб прогнозування, навіть з використанням квантових комп'ютерів.

Порівняння характеристик захищеності QRNG та класичних алгоритмічних PRNG приведено в табл. 1.

Таблиця 1

Параметр	QRNG	PRNG
Стійкість до прогнозування	Максимальна	Уразливий до підбору
Вплив бічних каналів	Існує	Обмежений
Фізичний рівень захисту	Необхідний	Мінімальний
Чутливість до середовища	Висока	Низька

Застосування веб-сервісів QRNG стало критично важливим для забезпечення безпеки банківських систем, інтернету речей та інших високочутливих платформ. Наприклад, при шифруванні даних QRNG виступають як надійний інструмент для створення криптографічних ключів. Однак їх інтеграція в реальні системи породжує нові ризики, пов'язані з потенційними атаками на апаратному та програмному рівнях.

Важливим аспектом є ризик атак на QRNG через криптографічні бібліотеки, які можуть бути вразливими до зовнішнього втручання або маніпуляцій на рівні програмного забезпечення. Наприклад, неправильна реалізація екстрактора QRNG у бібліотеках типу OpenSSL може стати причиною генерації передбачуваних чисел, що піддає загрозі всю систему. Зловмисники можуть скористатися цією вразливістю для перехоплення сеансових ключів або доступу до зашифрованих даних.

Ще одним критичним вектором атак є маніпуляція середовищем виконання, що може призводити до спотворення результатів QRNG під час генерації чисел. Якщо зловмисники отримають доступ до програмного середовища, вони зможуть змінювати вихідні значення QRNG, тим самим створюючи криптографічно слабкі ключі.

Крім програмних атак, QRNG також можуть бути вразливими до апаратних дефектів або збоїв під час інтеграції на фізичному рівні. Наприклад, дефекти мікросхем або некоректне налаштування апаратного забезпечення можуть призводити до збоїв у генерації ключів. У випадках масштабних веб-сервісів або хмарних платформ ці ризики є особливо критичними, оскільки навіть незначна похибка може призвести до масштабних витоків даних.

Важливо враховувати і атаки через бічні канали, що використовують витік інформації із систем QRNG шляхом аналізу часу виконання, енергоспоживання або електромагнітних випромінювань. Такі атаки є складними для виявлення, але вони можуть надати зловмисникам цінну інформацію про вихідні дані генератора.

Метою статті є класифікація та аналіз основних типів атак на веб-сервіси QRNG, обґрунтування та дослідження ефективних методів їх запобігання. Основна увага приділяється програмним атакам, атакам через бічні канали та уразливостям апаратного рівня. Також роз-

глядаються сучасні методи захисту, такі як сертифікація QRNG, мультифакторна перевірка даних та алгоритми моніторингу, що дозволяють виявляти потенційні загрози в реальному часі.

1. Атаки на QRNG на програмному рівні

1.1. Атаки на криптографічні бібліотеки

Одним із найпоширеніших векторів атак на QRNG є компрометація криптографічних бібліотек, які забезпечують генерацію та обробку випадкових чисел для захищених з'єднань. Бібліотеки, такі як OpenSSL, використовуються для реалізації протоколів захисту мережевого трафіку, зокрема TLS (Transport Layer Security). Уразливості у цих бібліотеках можуть виникати через помилки в коді екстрактора QRNG або відсутність стандартизованих механізмів перевірки вихідних даних генератора в реальному часі.

Атака може бути здійснена шляхом підміни джерела випадкових чисел під час виконання криптографічних операцій [1]. Якщо бібліотека не виконує належної перевірки джерела генерації чисел, зловмисник може інтегрувати менш стійкий генератор, який дозволяє прогнозувати вихідні значення. У такому випадку TLS-з'єднання стає вразливим до атаки "людина посередині", що дозволить розшифрувати конфіденційні дані.

Ще одним прикладом є атака на рівні ініціалізації QRNG. Під час запуску криптографічної системи QRNG генерує первинні значення, які використовуються як сеансові ключі. Якщо зловмисники отримують доступ до цього етапу генерації, вони можуть маніпулювати ключами або перехоплювати їх до моменту шифрування. Уразливості такого типу часто виникають у результаті недостатньої ентропії на ранніх етапах генерації або внаслідок слабких початкових параметрів бібліотеки.

1.2. Маніпуляція середовищем виконання

Маніпуляція середовищем виконання коду екстрактора QRNG є критичним вектором атак, який дозволяє зловмисникам впливати на процес генерації чисел під час його роботи. Якщо програмне середовище недостатньо захищене або має недоліки в системі доступу, зловмисник може впровадити шкідливий код, що змінить поведінку екстрактора. Наприклад, шляхом ін'єкції коду на рівні операційної системи можливе перехоплення результатів генерації або створення навмисних збоїв у роботі QRNG.

Навіть мінімальні маніпуляції середовищем можуть мати катастрофічні наслідки для криптографічних систем, які залежать від QRNG [2]. Середовище виконання може піддаватися атакам під час віддалених оновлень програмного забезпечення, що дає можливість зловмисникам модифікувати налаштування екстрактора. Уразливості виникають через відсутність контрольних сум або механізмів перевірки цілісності файлів під час оновлення.

Ще одним аспектом є використання вразливостей системної пам’яті. Зловмисники можуть отримати доступ до регістрів QRNG або буферів даних і підмінити вихідні значення випадкових чисел. Такий підхід дозволяє створити передбачувані ключі шифрування, що значно знижує рівень безпеки системи.

1.3. Атаки бічними каналами (Side-channel attacks)

Атаки бічними каналами є одним із найбільш витончених типів атак на QRNG. Вони базуються на аналізі непрямих фізичних характеристик системи під час генерації випадкових чисел, таких як споживання енергії, час виконання операцій, електромагнітне випромінювання або тепловий вплив. Ці фактори можуть містити інформацію про внутрішні процеси QRNG, що дозволяє зловмиснику відновити частину або всі вихідні значення генератора.

Ймовірність успішної атаки через бічний канал можна розрахувати за формулою

$$P_{attack} = 1 - \left(1 - \frac{E_{leak}}{E_{total}}\right)^n, \quad (1)$$

де E_{leak} – кількість енергії, що витікає з QRNG; E_{total} – загальна енергія процесу генерації, n – кількість спроб атаки.

Атаки бічними каналами можуть бути реалізовані навіть на рівні захищених систем із фізичним захистом QRNG [3]. Використання високочутливих датчиків дозволяє аналізувати найдрібніші коливання напруги або температури, що створює можливості для витоку даних. Наприклад, QRNG, що використовують фотонні технології, можуть піддаватися атакам через аналіз випромінювання лазерів або зміну інтенсивності світла.

Щоб мінімізувати ризики таких атак, виробники QRNG впроваджують механізми маскування даних, які додають випадкові шуми або спотворюють фізичні характеристики під час генерації чисел. Проте, ці методи не завжди є ефективними проти сучасних бічних атак, що використовують машинне навчання для аналізу навіть прихованих закономірностей.

Таким чином, атаки на QRNG на програмному рівні є серйозною загрозою для криптографічних систем. Ефективний захист QRNG вимагає комплексного підходу, який включає сертифікацію криптографічних бібліотек, контроль середовища виконання та захист від атак через бічні канали.

2. Уразливості на рівні інтеграції

2.1. Атаки через апаратну інфраструктуру

Інтеграція QRNG на апаратному рівні є важливим, але водночас вразливим етапом у забезпеченні криптографічної безпеки веб-сервісів. Уразливості можуть виникати в результаті фізичних дефектів апаратного забезпечення або недостатньо ретельної перевірки під час виробництва QRNG-чипів. Зловмисники можуть реалізовувати атаки через використання дефектних або підроблених компонентів, що мають вбудовані "бекдори" або інші приховані механізми [4].

Ці "бекдори" можуть активуватися під час криптографічних операцій, надаючи зловмиснику доступ до процесу генерації чисел або навіть можливість підміняти вихідні значення QRNG. Наприклад, у випадку інтеграції QRNG в процесори або мікроконтролери, зловмисники можуть зчитувати частину вихідних ключів через специфічні команди на рівні апаратного інтерфейсу. Такі атаки надзвичайно складно виявити, оскільки вони не залишають видимих слідів на програмному рівні.

Крім того, QRNG можуть бути вразливими до атак типу фізичного доступу. Наприклад, у випадку зламів дата-центрів або фізичного вторгнення до серверних кімнат, зловмисники можуть підміняти QRNG або вбудовувати шкідливі компоненти, які перехоплюють криптографічні ключі під час їхньої генерації. Для мінімізації таких ризиків необхідно впроваджувати багаторівневий контроль обладнання, включаючи регулярну перевірку QRNG за допомогою тестування на сторонні компоненти та приховані модифікації.

2.2. Апаратні дефекти і збої

Апаратні дефекти та збої можуть виникати як на етапі виробництва QRNG, так і під час їхньої експлуатації. Навіть найменші відхилення у процесі виготовлення мікросхем можуть спричинити зниження рівня випадковості, що робить генератор менш надійним для криптографічних задач. QRNG, інтегровані в хмарні обчислювальні системи, можуть піддаватися ризику часткової деградації апаратних компонентів через тривале навантаження або температурні перепади [5].

У таких випадках генератор може видавати некоректні або повторювані значення, що критично знижує криптографічну стійкість системи. Крім того, можливі перебої в електропостачанні або помилки у зв'язку між компонентами QRNG та іншими модулями системи, що може призвести до неповного або пошкодженого процесу генерації чисел.

Для виявлення таких дефектів важливо впроваджувати системи самодіагностики QRNG, які можуть виявляти будь-які відхилення у вихідних даних генератора. Наприклад, регулярна перевірка вихідних чисел на предмет відповідності статистичним критеріям випадковості до-

зволяє оперативно ідентифікувати деградацію апаратного забезпечення. Крім того, розробка резервних механізмів генерації дозволяє миттєво замінювати пошкоджені QRNG, запобігаючи можливості витоків даних.

2.3. Інтеграційні конфлікти з іншими компонентами системи

QRNG часто інтегруються з іншими криптографічними компонентами, такими як традиційні PRNG або системи шифрування на основі апаратних модулів безпеки (Hardware Security Modules, HSM). У таких випадках можливі конфлікти між вихідними значеннями QRNG та іншими генераторами, що може призвести до помилок у криптографічних алгоритмах або навіть повної втрати ентропії. Некоректна конфігурація системи може призвести до зниження рівня випадковості вихідних чисел, оскільки QRNG і PRNG можуть працювати паралельно без належної синхронізації [6].

Додатковим ризиком є конфлікт протоколів передачі даних. У деяких випадках QRNG передають вихідні значення через загальні канали зв’язку, які можуть бути перехоплені або модифіковані. Це створює можливість для атаки підміни вихідних чисел на рівні передачі даних між компонентами системи.

Для захисту від таких атак, необхідно впроваджувати ізольовані канали передачі даних між QRNG та криптографічними бібліотеками, а також застосовувати механізми апаратної автентифікації генератора. Також доцільно використовувати алгоритми перевірки сумісності компонентів та регулярне оновлення системного програмного забезпечення, щоб забезпечити коректну роботу QRNG у комплексних криптографічних системах.

Таким чином, інтеграція QRNG на апаратному рівні створює численні виклики, які потребують детального аналізу та впровадження багаторівневих механізмів захисту. Підходи, що включають регулярну перевірку обладнання, діагностику та ізольовані канали передачі даних, є важливими для забезпечення надійності QRNG у сучасних криптографічних системах.

3. Механізми захисту QRNG від атак

3.1. Валідація та сертифікація QRNG

Валідація та сертифікація QRNG є критичними етапами для гарантування їхньої надійності та стійкості до атак. Ці процеси дозволяють не лише підтвердити відповідність QRNG міжнародним стандартам, але й виявити потенційні вразливості до моменту інтеграції в реальні системи. Важливим елементом є багатоступенева перевірка QRNG як на етапі виробництва, так і в процесі експлуатації.

Процес сертифікації включає кілька рівнів:

1. Тестування випадковості – перевірка QRNG на відповідність критеріям випадковості та статистичним тестам, таким як NIST SP800-90, Dieharder та тест Фур'є-аналізу.

2. Перевірка на фізичні дефекти – аналіз мікросхем QRNG на наявність потенційних апаратних дефектів або вразливостей, які можуть вплинути на генерацію чисел.

3. Програмна сертифікація – тестування програмного забезпечення, яке обробляє вихідні дані QRNG, з метою виявлення вразливостей на рівні алгоритмів.

Оскільки нові методи атак постійно розвиваються, регулярне оновлення сертифікаційних стандартів для QRNG є важливим. Сертифікація має відбуватися в умовах реальних навантажень і включати сценарії атаки через бічні канали, апаратні збої та спроби компрометації середовища виконання.

Крім того, впровадження систем аудиту та постійного моніторингу QRNG дозволяє своєчасно виявляти потенційні відхилення у генерації випадкових чисел. Наприклад, якщо генератор демонструє повторюваність чисел або знижує рівень випадковості, система автоматично сигналізує про необхідність заміни чи повторної сертифікації генератора.

3.2. Мультифакторна перевірка даних

Мультифакторна перевірка є ключовим механізмом підвищення стійкості QRNG до атак та апаратних збоїв. Вона передбачає використання кількох незалежних джерел випадкових чисел для перевірки коректності вихідних даних. У разі розбіжності між джерелами генерації система автоматично блокує подальшу обробку чисел або ініціює повторну генерацію.

Одним із прикладів такої практики є інтеграція QRNG із традиційними PRNG для перевірки відповідності вихідних значень. У такій системі QRNG виконує основну функцію генерації ключів, тоді як PRNG працює як резервний механізм для перевірки статистичних закономірностей.

В роботі [8] представлена гібридна модель, у якій QRNG працює спільно із квантовою ключовою дистрибуцією (Quantum Key Distribution, QKD). Цей підхід дозволяє значно підвищити рівень безпеки, оскільки навіть якщо QRNG буде скомпрометований, QKD забезпечить захист каналів передачі ключів.

Крім того, мультифакторна перевірка включає:

1. Контроль фізичних параметрів QRNG, таких як температура, рівень енергоспоживання та стабільність вихідних даних.

2. Використання кількох QRNG в одній системі з подальшим порівнянням результатів між генераторами.

3. Інтеграція з апаратними модулями безпеки (HSM), які виконують додаткові перевірки та захищають QRNG від зовнішніх атак.

3.3. Моніторинг та виявлення аномалій

Моніторинг та виявлення аномалій є невід'ємною частиною комплексної системи захисту QRNG. Оскільки атаки на QRNG можуть бути як програмними, так і фізичними, необхідно використовувати багаторівневі методи аналізу, які дозволяють виявляти будь-які відхилення у роботі генератора на різних етапах його функціонування.

Системи моніторингу QRNG спрямовані на контроль вихідних даних генератора, аналіз фізичних характеристик генератора, виявлення стороннього втручання та запобігання апаратним збоям. Ці механізми мають бути адаптовані до специфіки QRNG, оскільки квантові процеси є надзвичайно чутливими до зовнішніх факторів, таких як зміни температури, електромагнітні поля або шум.

Також є важливим впровадження алгоритмів машинного навчання (machine learning, ML) для аналізу вихідних даних QRNG у реальному часі [9]. Такі алгоритми здатні виявляти приховані закономірності або повторення у вихідних числах, які можуть бути ознакою компрометації генератора.

До ключових методів моніторингу належать:

1. Аналіз фізичних параметрів генерації чисел.

Моніторинг фізичних параметрів QRNG дозволяє виявити відхилення, які можуть свідчити про можливу атаку або апаратний дефект. Наприклад, зміни в енергоспоживанні або теплових характеристиках QRNG можуть вказувати на атаку через бічні канали або спробу маніпуляції середовищем виконання.

Для підвищення ефективності цього підходу використовуються:

– датчики температури та енергоспоживання, які постійно фіксують дані про роботу QRNG. У разі виявлення відхилень система автоматично переходить у режим діагностики або аварійного відключення.

– спектральний аналіз сигналів QRNG, що дозволяє виявляти частотні відхилення та приховані закономірності у процесі генерації чисел.

2. Часовий аналіз та аналіз продуктивності QRNG

Моніторинг продуктивності QRNG включає аналіз часу генерації чисел та перевірку відповідності вихідних даних заданим криптографічним стандартам. Якщо генератор почи-

нає працювати повільніше або, навпаки, демонструє надто швидку генерацію чисел, це може свідчити про внутрішні збої або зовнішнє втручання.

Особливу увагу слід приділяти:

– затримкам у генерації чисел, що можуть бути ознакою атаки на рівні програмного забезпечення.

– раптовим змінам у швидкості генерації ключів, які можуть свідчити про спробу підміни QRNG або маніпуляції апаратними компонентами.

3. Використання штучного інтелекту (Artificial Intelligence, AI) для моніторингу QRNG

Одним із найперспективніших напрямків у галузі моніторингу QRNG є використання алгоритмів машинного навчання (ML) та штучного інтелекту (AI). AI може аналізувати великі обсяги даних та виявляти приховані закономірності, які не піддаються класичним методам аналізу.

Алгоритми глибокого навчання (DL) здатні навчатися на історичних даних QRNG і виявляти навіть найдрібніші відхилення у вихідних числах або фізичних характеристиках генератора. У разі виявлення аномалій AI може автоматично ініціювати перехід на резервний QRNG або заблокувати компрометований генератор.

Крім того, AI-системи можуть проводити:

– автоматичний аналіз кореляцій вихідних чисел, що дозволяє виявляти повторюваність або закономірності у генерації випадкових чисел.

– детекцію аномалій у реальному часі, яка дозволяє миттєво реагувати на будь-які відхилення у роботі генератора.

4. Автоматизовані системи аварійного моніторингу

Важливим компонентом є впровадження автоматизованих систем аварійного моніторингу QRNG, які працюють у безперервному режимі та миттєво реагують на виявлення підозрілих процесів.

Автоматизовані системи моніторингу включають:

– резервні генератори (Backup QRNG), які активуються у разі виявлення дефектів в основному генераторі.

– аварійне відключення QRNG з подальшим аналізом та діагностикою виявлених проблем.

– логування всіх операцій генератора для подальшого аудиту та аналізу на предмет можливих атак або збоїв.

Моніторинг QRNG має бути інтегрований у загальну систему кібербезпеки організації. Це дозволяє синхронізувати дані з інших компонентів безпеки та виявляти комплексні атаки, які можуть поєднувати програмні, апаратні та фізичні вектори загроз.

Наприклад, система моніторингу QRNG може взаємодіяти з системами управління подіями та інцидентами (SIEM), які забезпечують централізований збір та аналіз даних про безпеку.

Моніторинг QRNG є не лише засобом виявлення аномалій, але й інструментом для довготривалої оцінки ефективності системи. Виявлення поступової деградації апаратних компонентів або зниження рівня ентропії генератора дозволяє своєчасно вжити заходів щодо заміни або оновлення обладнання.

Таким чином, комплексний підхід до моніторингу QRNG, що включає фізичний аналіз, часовий контроль, використання AI та інтеграцію з іншими системами безпеки, забезпечує високий рівень стійкості квантових генераторів до сучасних загроз та атак.

3.4. Автоматизація захисних механізмів

Окремим напрямом розвитку захисних механізмів QRNG є впровадження автоматизованих систем захисту, які здатні самостійно реагувати на аномалії та ініціювати процеси аварійної зупинки генерації чисел або перехід на резервний генератор.

Ключові елементи автоматизації:

– система швидкої заміни QRNG – резервні генератори підключаються до системи миттєво після виявлення аномалій, що забезпечує безперервність генерації чисел.

– автономне оновлення сертифікації – генератор автоматично проходить перетестування після критичних оновлень програмного забезпечення або виявлення потенційних загроз.

– дистанційний контроль – можливість віддалено відключати або перезавантажувати QRNG у разі виявлення фізичних атак або підозрілих процесів.

Завдяки впровадженню таких автоматизованих систем, QRNG стають значно менш вразливими до атак як на програмному, так і на апаратному рівнях.

Таким чином, комплексний підхід до захисту QRNG включає в себе сертифікацію, мультифакторну перевірку та постійний моніторинг. Усі ці елементи дозволяють значно підвищити стійкість квантових генераторів до сучасних атак та забезпечити їхню надійну інтеграцію в криптографічні системи майбутнього.

Висновки

Впровадження QRNG в системи захисту інформації супроводжується низкою викликів, які можуть призвести до серйозних загроз для безпеки даних. У цій роботі були розглянуті потенційні вразливості QRNG на програмному рівні, під час інтеграції та на рівні апаратного забезпечення.

Атаки на QRNG на програмному рівні залишаються одним із найпоширеніших векторів загроз. Зловмисники можуть використовувати вразливості криптографічних бібліотек, маніпулювати середовищем виконання або здійснювати атаки через бічні канали, що призводить до витоку ключів або компрометації вихідних даних. Недостатній захист програмного середовища або відсутність механізмів моніторингу якості QRNG може стати причиною серйозних проблем у роботі систем кіберзахисту.

Атаки на рівні інтеграції QRNG в апаратне забезпечення створюють додаткові загрози, оскільки навіть найменші дефекти мікросхем або неправильно налаштовані системи можуть суттєво знизити рівень випадковості вихідних чисел. Фізичний доступ до QRNG відкриває можливості для зловмисників впровадити апаратні закладки або модифікації, що ускладнює виявлення атак стандартними методами.

Особливу увагу слід приділяти атакам через бічні канали. Ці атаки використовують фізичні параметри роботи QRNG, зокрема енергоспоживання, теплові відхилення або електромагнітні сигнали, щоб отримати інформацію про вихідні дані генератора. Подібні атаки важко виявити та зупинити, оскільки вони не залишають цифрових слідів і експлуатують фізичні характеристики системи.

Для мінімізації цих загроз необхідно впроваджувати комплексні захисні механізми на всіх рівнях роботи QRNG. Важливим етапом є валідація та сертифікація QRNG з дотриманням міжнародних стандартів. Цей процес дозволяє гарантувати, що генератор працює коректно і відповідає вимогам криптографічної безпеки. Регулярне тестування, аналіз статистичної випадковості та виявлення фізичних дефектів забезпечують стабільність роботи генератора в реальних умовах.

Додатковий рівень захисту забезпечується за рахунок мультифакторної перевірки вихідних даних, яка використовує кілька незалежних джерел випадковості для перевірки QRNG. Поєднання QRNG із традиційними PRNG або QKD дозволяє мінімізувати ризики, пов’язані з компрометацією одного джерела генерації.

Важливим компонентом є системи моніторингу та виявлення аномалій, які дозволяють виявляти потенційні відхилення у роботі QRNG у режимі реального часу. Використання алгоритмів машинного навчання та штучного інтелекту для аналізу вихідних даних генератора підвищує ефективність захисту та дозволяє оперативно реагувати на загрози. Постійний моніторинг фізичних параметрів роботи QRNG допомагає виявити спроби атак через бічні канали або апаратні дефекти.

Окремим напрямом є автоматизація захисних механізмів, яка дозволяє автоматично перемикати генератори, перезавантажувати систему або здійснювати аварійну зупинку генерації чисел у разі виявлення аномалій. Це дозволяє зменшити час реакції на загрози та гарантувати безперебійну роботу систем шифрування.

У перспективі розвиток квантових обчислень та квантових комунікаційних систем потребуватиме вдосконалення QRNG та впровадження нових стандартів безпеки. Інтеграція QRNG із квантовими комп'ютерами та квантовими мережами дозволить створити більш стійкі до атак криптографічні системи. Водночас, це створить нові виклики, пов'язані з необхідністю захисту квантових систем від фізичних та апаратних атак.

Впровадження QRNG у веб-сервіси та критичні інфраструктури потребує комплексного підходу до захисту, який поєднує сертифікацію, мультифакторну перевірку, моніторинг та автоматизацію захисних механізмів. Такий підхід дозволить значно знизити ризики та забезпечити максимальний рівень безпеки для криптографічних систем.

Список літератури:

1. Blanco-Romero J., Lorenzo V., & Almenares F. Evaluating integration methods of a quantum random number generator in OpenSSL for TLS // Computer Networks. 2024. Vol 255, article №110877. doi:10.1016/j.comnet.2024.110877
2. Henry Elizabeth. (2024). The Role of Quantum Random Number Generation in Enhancing Encryption Security. SSRN, doi:10.2139/ssrn.4966139
3. Regazzoni F., et al. (2021). A high speed integrated quantum random number generator with on-chip real-time randomness extraction. doi:10.48550/arXiv.2102.06238
4. Bishwas A. K., & Sen M. (2024). Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat. doi:10.48550/arXiv.2411.09995
5. Pedone I., et al. (2021). Toward a complete software stack to integrate quantum key distribution in a cloud environment // IEEE Access. doi:10.1109/ACCESS.2021.3102313
6. Adetifa, O. E. Comparative Analysis and Applications of Quantum Random Number Generators: Evaluating Efficiency, Statistical Properties, and Real-world Use Cases // Morgan State University. ProQuest Dissertations & Theses, 2024. 31141646. link https://www.proquest.com/openview/0e228ff803da898521302a83a2d3b7d4 preview lang Eng
7. Mehmood A., et al. (2024). Advances and vulnerabilities in modern cryptographic techniques // IEEE Access. doi:10.1109/ACCESS.2024.3367232
8. Huang L., et al. A practical hybrid quantum-safe cryptography scheme between data centers // Proceedings Volume 11540, Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defence III; 1154008. 2020. doi:10.1117/12.2573558
9. Cherbal S., Zier A., Hebal S. et al. Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing // J. Supercomput. 2024. Vol. 80. P. 3738–3816. doi:10.1007/s11227-023-05616-2

Надійшла до редколегії 09.01.2025

Відомості про авторів:

Моргуль Дмитро Миколайович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій; Україна; e-mail: dmitriymdn85@gmail.com; ORCID: https://orcid.org/0009-0007-5272-1634

Нарєжній Олексій Павлович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій; Україна; e-mail: o.nariezhnii@karazin.ua; ORCID: https://orcid.org/0000-0003-4321-0510

Гріненко Тетяна Олексіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій; Україна; e-mail: tetiana.grinenko@nure.ua; ORCID: https://orcid.org/0000-0002-8251-8991