УДК 004.056 **DOI:10.30837/rt.2025.3.222.06**

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

РОЗРОБКА ТИПОВОЇ ІНФРАСТРУКТУРИ ДЛЯ ВЕБ-СЕРВІСУ КВАНТОВОГО ГЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ

Вступ

Квантові генератори випадкових чисел (QRNG, quantum random number generator) є критично важливими для забезпечення високої ентропії у криптографічних системах, моделюванні та наукових дослідженнях. Локальні рішення гарантують максимальну безпеку, але не завжди доступні через вартість і технічні обмеження. Публічні веб-сервіси QRNG, що надають доступ до квантової випадковості через інтерфейс прикладного програмування (API, application programming interface), дозволяють швидко інтегрувати її у прототипи, навчальні проєкти та дослідницькі системи. Водночас відсутність уніфікованого підходу до інфраструктури таких сервісів ускладнює їх порівняння, інтеграцію та аудит.

Сучасні веб-сервіси ґрунтуються на високоякісній випадковості для криптографічних протоколів, керування сесіями, токенів доступу, seed-значень і моделювання. Криптографічно стійкі детерміновані генератори випадкових бітів (DRBG, deterministic random bit generator) критично залежать від секретності початкових станів і коректності реалізації, тоді як істинно випадкові генератори (TRNG, true random number generator) можуть зазнавати систематичних похибок або деградації джерела ентропії. QRNG, які відносяться до TRNG, вирізняються тим, що спираються на фундаментальну невизначеність вимірювань у квантовій механіці, забезпечуючи принципово непередбачувану ентропію за умови коректної побудови вимірювальної схеми та постобробки [1, 2]. Питання інтеграції QRNG як мережевого сервісу (веб-сервісу QRNG) є актуальною задачею масштабування довіри до випадковості для широкого кола прикладних напрямків – від критичної інфраструктури держави до кібербезпеки хмарних платформ.

Перехід до формату веб-сервісу породжує нові ризики і вимоги [3]. По-перше, джерело ентропії має бути фізично надійним та валідованим відповідно до процедур оцінювання min-ентропії відповідно до рекомендацій NIST SP 800-90B щодо створення моделі джерела ентропії, контролю якості бітів і виявлення відмов [4]. По-друге, результати екстракції повинні мати гарантії наближення до рівномірного розподілу. На практиці для QRNG часто використовують екстрактори на основі Toeplitz-гешування та пов’язане з ними доведення через LHL (Leftover Hash Lemma) [5]. Наприклад, для реалізації високих сервісних навантажень використовується апаратна реалізація типу FPGA-based Toeplitz Strong Extractor для QRNG [6]. По-третє, навіть за правильної екстракції потрібно здійснювати health-тести (continuous tests) вихідних потоків джерела ентропії за допомогою рекомендацій NIST SP 800-90B [4].

Мета статті – розробити та обґрунтувати типову інфраструктуру веб-сервісу QRNG, яка включатиме функціональні компоненти, вимоги до безпеки, інтерфейси доступу (API), методи контролю якості випадковості та рекомендації щодо масштабування. Запропонована інфраструктура має слугувати основою для створення сумісних, безпечних і продуктивних веб-сервісів джерел квантової ентропії.

1. Вимоги до типової інфраструктури публічного веб-сервісу QRNG

Із погляду безпеки потоку даних веб-сервісу QRNG потрібно використовувати TLS 1.3 з мінімізацією поверхні атаки [7]. Для цифрової ідентифікації користувача на веб-сервісі QRNG пропонується керуватися вимогами NIST SP 800-63B-4 [8] щодо життєвого циклу автентифікаторів і застосовувати біометрію у складі багатофакторної автентифікації (MFA, multi-factor authentication). Для авторизації та делегування доступу пропонується використовувати протокол OAuth 2.0 з короткоживучими токенами та форматом JWT (JSON Web Token) для перенесення підписаних повноважень [9, 10]. На рівні периметра

інфраструктура має забезпечувати відокремлення зон (демілітаризовані зони (DMZ, demilitarized zone), підмережі для бекендів і сховищ), передбачувану поведінку NAT (Network Address Translation) і Internet-gateway та контрольований вихідний трафік через керований вихідний проксі згідно з відповідними RFC-вимогами [11 – 14].

Теоретичні моделі довіри до QRNG також еволюціонують. Поряд із класичною (повністю довіреною) моделлю популярності набувають незалежний від джерела (SI, source-independent) та незалежний від пристрою (DI, device-independent) підходи, де випадковість може бути сертифікована експериментально через порушення нерівностей Белла навіть за обмеженої довіри до елементів апаратури [15 – 18]. У роботі [19] демонструється суттєвий прогрес у швидкостях DI-генерації з одночасною сертифікацією квантової випадковості, що поступово знімає бар'єри до використання таких схем у сервісних сценаріях. У дослідженні розглянуто SI/DI як цільові напрями розвитку QRNG і показано, як закласти для них «каркас» у типовій інфраструктурі без шкоди для продуктивності поточної (класичної) реалізації [19].

Узагальнюючи, дослідницька задача цієї роботи полягає у побудові типової інфраструктури веб-сервісу QRNG, яка задовольняє наступним вимогам:

1. Гарантує обґрунтовану якість випадковості через моделювання джерела, коректну екстракцію та статистичну валідацію [4 – 6, 20].

2. Забезпечує сучасний захист комунікації, ідентифікацію та делегування доступу (TLS 1.3; NIST SP 800-63B-4; OAuth 2.0/JWT) [7 – 10].

3. Мінімізує периметрові ризики і контролює вихідні потоки (NAT, Internet-gateway, outbound-proxy) [11 – 14].

4. Має чітку дорожню карту постквантової міграції відповідно до FIPS 203, FIPS 204, FIPS 205 і супровідних рекомендацій NIST [17, 21 – 24].

5. Допускає поступову інтеграцію SI/DI-сертифікації без радикальної перебудови всієї системи [5, 15 – 19].

2. Функціональна схема типової інфраструктури веб-сервісу QRNG та опис основних елементів

На рис. 1 наведена запропонована функціональна схема типової інфраструктури веб-сервісу QRNG.

Опис основних елементів функціональної схеми типової інфраструктури веб-сервісу QRNG та їх функції:

1. Internet-gateway і 15. NAT-gateway.

Internet-gateway забезпечує керований вихід/вхід трафіку між локальною мережею і мережею інтернет. NAT-gateway транслює приватні адреси, маскуючи внутрішній простір і дозволяючи масштабовану вихідну комунікацію. Поведінкові вимоги до NAT для UDP/TCP формалізовані в RFC 4787 та RFC 5382, а базова термінологія в RFC 2663; оновлення вимог наведено в RFC 7857 [11 – 13,25]. Для веб-сервісу QRNG це критично, оскільки згенерована на бекенді телеметрія, оновлення прошивки екстракторів мають виходити предиктивно, без витоку внутрішньої адресації.

2. Локальна мережа (зонування) (Local Network).

Сегментація на підмережі (DMZ для веб-сервісу; окремі VLAN/VPC-підмережі для QRNG-бекенду та сховищ) мінімізує бічний рух у разі компрометації. Завершення TLS розміщується або на edge-проксі, або безпосередньо у веб-сервісі з примусовою підтримкою TLS 1.3.

3. Модуль автентифікації (біометрія як фактор) (Authentication module (Biometric)).

Користувацька автентифікація (оператори, інтегратори, адміністратори веб-сервісу QRNG) реалізується відповідно до NIST SP 800-63B-4 (Authentication Assurance Level 2 та Level 3) [8]. Біометричні фактори можуть використовуватися у складі багатофакторних схем, але потребують управління життєвим циклом автентифікаторів, захисту шаблонів і валідації

придатності каналів (вимоги NIST SP 800-63B-4 щодо Authentication Assurance Level, Presentation Attack Detection (PAD) – загроз тощо).

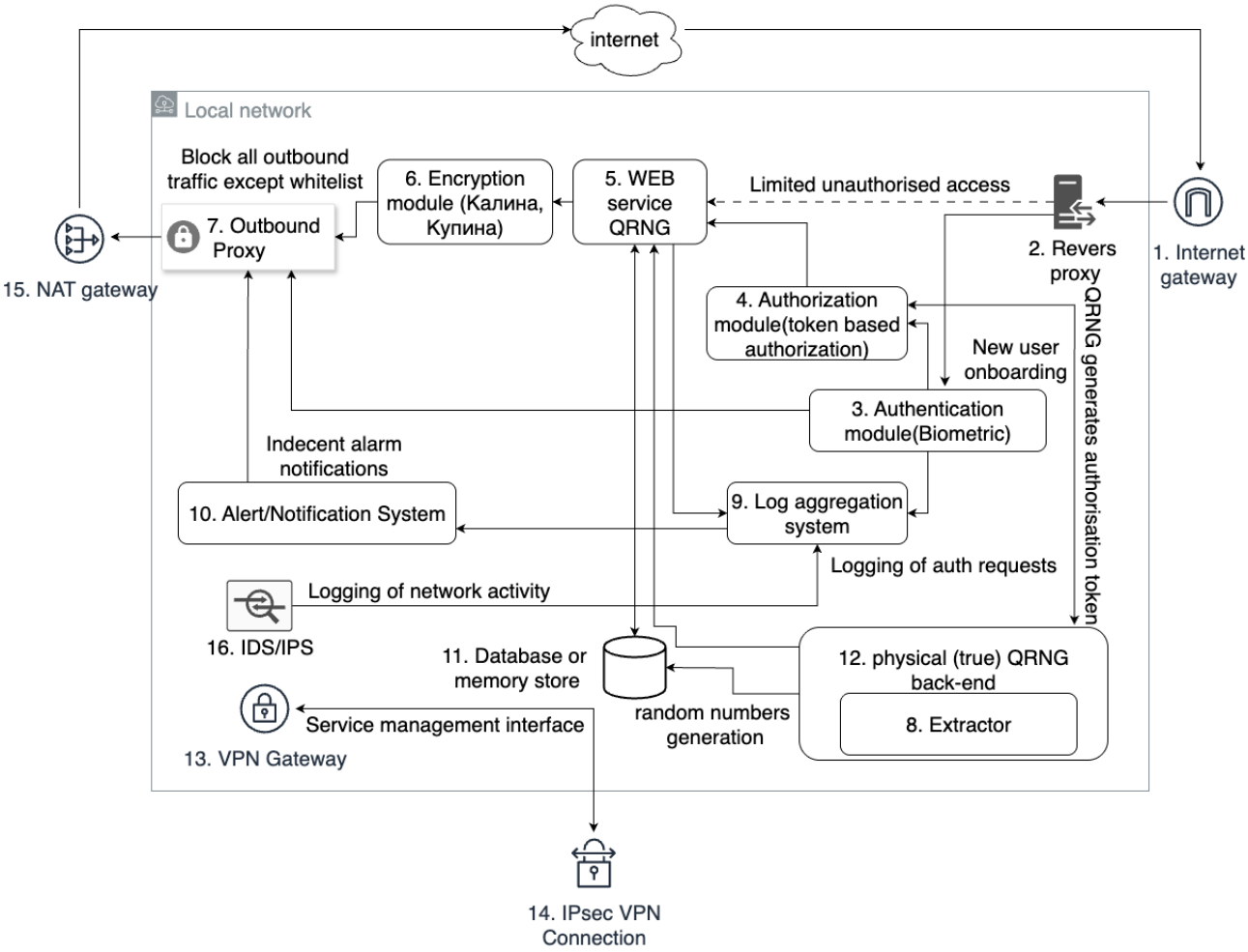

Рис. 1. Функціональна схема типової інфраструктури веб-сервісу QRNG

4. Модуль авторизації (токен-базована авторизація) (Authorization module (token based authorization)).

Внутрішній Authorization Server реалізує протокол OAuth 2.0 (RFC 6749) з видачею короткоживучих токенів доступу. Ресурси приймають токени у форматі JWT (RFC 7519) з відповідною політикою електронних підписів (RSASSA-PSS та ECDSA або постквантові варіанти «гібридних» токенів у перехідний період) [9, 10]. Для машинних інтеграцій рекомендується використання сервісних аккаунтів із обмеженим рівнем доступу, для користувачів – авторизаційний код відповідно протоколу OAuth 2.0 (PKCE, Proof Key for Code Exchange).

5. Веб-сервіс QRNG (API/портал) (WEB service QRNG).

Функціональність: запит на отримання бітів, параметри постобробки (екстракції), довідкова телеметрія (обчислення min-ентропії, температурні сенсори, оптичні сенсори), опціональний «віртуальний пул» з буферизацією. Для міжсервісної взаємодії обов'язкове використання TLS 1.3 з взаємною автентифікацією [7]. Підрахунок запитів контролюється через обмеження швидкості і квоти; аудиторські події фіксуються в журналі.

6. Модуль шифрування (дані під час передачі/дані на носіях) (Encryption module (Калина, Купина)).

Під час передачі даних використовується TLS 1.3. Дані на носіях шифруються за допомогою апаратних модулів HSM (Hardware Security Module) або KMS (Key Management Service). В умовах Української юрисдикції необхідно використовувати національні стандарти (наприклад, блоковий симетричний шифр «Калина» та геш-функція «Купина»).

7. Вихідний проксі (Outbound Proxy).

Всі вихідні HTTP(S)-потоки веб-сервісу QRNG (оновлення прошивок, залежності тощо) прямують через керований проксі з TLS-інспекцією, а також з обмеженням цільових доменів/підмереж. Таке обмеження сприяє інформаційному контролю потоків і відповідає загальним практикам захисту мережі, доповнюючи NAT-рівень.

8. Буфер постобробки/екстракції випадковості (Extractor).

Raw-біти QRNG піддаються оцінюванню min-ентропії відповідно до NIST SP 800-90B та екстракції для отримання рівномірного розподілу [4]. Інформаційно-теоретично доведена екстракція реалізується Toeplitz-гешуванням LHL, яке широко використовується в QRNG-реалізаціях і може бути апаратно прискорене (FPGA/SoC) [5, 26]. Оперативна перевірка вихідних даних після екстракції проводиться за допомогою статистичних тестів NIST SP 800-22.

9. Система агрегації логів (Log aggregation system).

Це програмне рішення, яке збирає, фільтрує, трансформує та об'єднує журнали (логі) з різних джерел (серверів, додатків, мережевих пристроїв) в єдину систему для спрощення аналізу та моніторингу. Журнали автентифікації, авторизації, запити API, телеметрія QRNG, результати тестів випадковості та адміністративні дії централізовано збираються і зберігаються згідно з встановленим періодом зберігання та Hot/Worm-політиками. Це забезпечує відтворюваність і ланцюжок довіри для аудитів (відповідність вимогам до обліку доступу, реагування на інциденти та розслідуваня).

10. Система оповіщення та нотифікацій (Alert/Notification System).

Це механізм для миттєвого інформування адміністраторів веб-сервісу про події (тригери), новини, оновлення чи критичні стани компонентів системи. Тригери на основі правил/кореляції (зниження min-ентропії нижче порогів SP 800-90B; аномальний rate API; невдачі TLS-перевірок; відхилення параметрів діода/лазера) сповіщають адміністраторів. Сповіщення надсилаються через надійні канали (залежно від політики ризику – через зашифровані канали або внутрішній мессенджер).

11. Сховище метаданих/«пулу» бітів (Database or memory store).

Пул зберігає попередньо екстраговані біти з криптографічним контролем цілісності та мітками часу/джерела. Політика «не повторювати» забезпечується індексуванням блоків/посиланням на «вичерпані» сегменти. Для зовнішніх клієнтів краще надавати потоки «на вимогу» без довготривалого зберігання.

12. Фізичний (істинний) QRNG-бекенд (physical (true) QRNG back-end).

Оптичні, фазові, вакуумні флуктуації чи інші квантові джерела ентропії генерують raw-біти, при цьому моніториться стан середовища джерела ентропії. Для доведеної безпекової моделі розглядаються підходи SI і DI, де випадковість може бути сертифікована навіть за обмеженої довіри до компонентів.

13. VPN-шлюз (VPN Gateway) та 14. IPsec VPN-з’єднання (IPsec VPN Connection).

Операційний доступ інженерів, приватні інтеграції з довіреними партнерами та кластерний менеджмент можуть додатково ізолюватися через IPsec-тунелі між визначеними сегментами мереж.

16. Система виявлення і запобігання вторгненням (IDS/IPS).

IDS/IPS є окремим шаром контролю, що моніторить мережевий трафік і події елементів інфраструктури з метою виявлення зловмисної активності та негайного блокування. IDS/IPS охоплює широкий простір протоколів і поведінкових патернів таких як сканування, «бічний рух» (Lateral Movement), аномалії у TLS-рукостисканнях тощо. Понятійна база наведена у NIST SP 800-94 (IDPS) [27] і спосіб контролю SI-4 (System Monitoring) у NIST SP 800-53 Rev.5 [28], які рекомендують як мережеві, так і хостові сенсори з централізованою кореляцією подій.

3. Обґрунтування ефективності типової інфраструктури веб-сервісу QRNG

Квантова випадковість і довірена постобробка. Багаторічні огляди і сучасні результати підтверджують, що QRNG на основі квантових процесів (детекція фотонів, фазові флуктуації тощо) забезпечують фундаментально непередбачувану випадковість, якщо вимірювальна система належно модельована і контрольована [1, 2]. Для зменшення впливу класичного шуму та систематик використовують теоретично доведені екстрактори: Toeplitz-гешування разом із LHL гарантує, що вихідні дані мають розподіл близький до рівномірного за наявності достатньої min-ентропії [5, 26]. Використання підходів SI і DI гарантує, що випадковість може бути сертифікована експериментально, але це знизить вимоги довіри до апаратури [15 – 18]. Останні експерименти демонструють мегабітні DI-швидкості з одночасною сертифікацією квантової випадковості, що робить їх більш практичними для сервісних сценаріїв [19].

Оцінка джерела ентропії повинна виконуватися згідно з NIST SP 800-90B (моделювання джерела, збір raw-даних, оцінювання min-ентропії, виявлення збоїв) із подальшим статистичним тестуванням потоків (SP 800-22 Rev.1a) як додатковим санітарним бар'єром [4, 20]. Послідовність тестування NIST SP 800-90B → екстракція → NIST SP 800-22 є де-факто стандартним безпековим підходом щодо оцінки джерела квантової ентропії [4, 5, 20].

Захищений транспортний потік та ідентифікація. TLS 1.3 лімітує використання застарілих шифрів, забезпечуючи захищений канал між клієнтом і веб-сервісом QRNG [7]. Це особливо важливо під час передачі токенів доступу та потоків випадкових бітів. Політика ідентифікації відповідає NIST SP 800-63B-4, а саме: біометрія застосовується як частина MFA (Authentication Assurance Level 2 та Level 3), автентифікатори керуються протягом усього життєвого циклу, згодом відкликаються і ревалідовуються. Це підтримується технологічно через Fast Identity Online-сумісні автентифікатори або апаратні ключі, однак, саме NIST SP 800-63B-4 визначає вимоги щодо рівнів запевнення (Assurance Level) і політик відновлення.

Авторизація та делегування доступу. Авторизація та делегування доступу забезпечується протоколом OAuth 2.0. Це забезпечує стандартизоване делегування з різними потоками (авторизаційні коди разом з PKCE для інтерактивних клієнтів; клієнтські повноваження для server-to-server), а JWT надає компактний формат перенесення прав із електронним підписом та шифруванням [9, 10]. Для веб-сервісу QRNG важлива короткоживучість токенів, вузька сфера застосування, чітке обмеження швидкості на ключ або клієнта та аудит усіх дій.

Постквантова готовність. У постквантовий період на веб-сервісі QRNG необхідно використовувати стандарти типу FIPS 203, FIPS 204, FIPS 205 і супровідні матеріали NIST [17, 21 – 24]. Наприклад, ML-KEM для обміну ключами, а ML-DSA/SLH-DSA для електронних підписів.

Периметр і керування вихідним трафіком. NAT/Internet-gateway разом із outbound-proxy обмежують поверхню атак і створюють спостережний контроль за зовнішніми залежностями. Стандарти RFC 4787, RFC 5382, RFC 2663, RFC 7857 регламентують поведінку NAT, що забезпечує передбачуваність з'єднань.

Спостережність і відповідальність. Централізоване журналювання з кваліфікованою електронною позначкою часу (NTP autokey), що дозволяє відстежити інциденти: падіння min-ентропії, аномалії запитів, збої TLS, спроби перевищення квот. Це критично для відповідності вимогам кібербезпеки і для незалежної перевірки веб-сервісів QRNG.

Загрози і їх пом'якшення. Вихід з ладу джерела квантової ентропії: постійний моніторинг min-ентропії згідно з NIST SP 800-90B. Атака Man-in-the-Middle: використання TLS 1.3 разом з mTLS для міжсервісних зв'язків; суворий контроль SSL сертифікатів. Компрометація токенів: короткі життєві цикли, обмежені сфери застосування, ротація ключів електронного підпису JWT, аудит випуску токенів. Зловживання API: квотування, обмеження швидкості, розгалуження доступів відповідно бізнес моделі, відсікання аномалій. Апаратні збої: резервування джерела квантової ентропії; контроль допусків сенсорів; аварійний канал DRBG з

чітким маркуванням походження бітів (і забороною «змішування» без явної політики). Периметрові ризики: відмова від відкритих вихідних маршрутів, зазначені можливі маршрути через outbound-proxy, конфігурація NAT згідно з RFC 4787, RFC 6888, RFC 7857.

Висновки

Представлена інфраструктура веб-сервісу QRNG є типовою і має адаптуватися до галузевих та регуляторних вимог, зокрема, національної нормативно-правової бази в галузі кібербезпеки. Частина джерел про DI-генерацію залишається експериментальною, їх безшовна інтеграція у високонавантажені веб-сервіси QRNG потребує додаткових інженерних досліджень продуктивності й відмовостійкості. Оцінка економічного ефекту впровадження типової інфраструктури веб-сервісу QRNG у постквантовий період залежить від профілю клієнтів і життєвого циклу даних.

Напрями майбутніх робіт: по-перше, перспективним є створення відкритих апаратних (FPGA/SoC) еталонних наборів телеметрії QRNG для поточної оцінки джерела квантової ентропії згідно з рекомендаціями NIST SP-800-90B; по-друге, формалізація цілі рівня обслуговування та угоди про рівень надання послуг для веб-сервісів джерел квантової ентропії. Наприклад, гарантований min-ентропійний бюджет на запит та прозорість журналів аудиту. По-третє, розробка гібридних протоколів TLS з постквантовим рукостисканням, оптимізованих для навантажених REST API. Наприклад, використання апаратних прискорювачів екстракції (FPGA/SoC) з доведеними властивостями та відкритими описами проєктів.

Таким чином, запропонована інфраструктура веб-сервісу QRNG забезпечує збалансований компроміс між науковою обґрунтованістю, інженерною практичністю та регуляторною відповідністю. Вона дає організаціям чітку дорожню карту: від відомих прототипів QRNG з формальною екстракцією і сучасним стеком безпеки – до поступового впровадження SI/DI-сертифікації та повної постквантової готовності. Такий підхід дозволяє підвищити рівень довіри до веб-постачання випадкових бітів з джерел квантової ентропії і зробити цей ресурс надійним фундаментом для широкого спектра криптографічних та прикладних задач у майбутньому.

Список літератури:

1. Ma X., Yuan X., Cao Z., Qi B., and Zhang Z. Quantum random number generation // Quantum Information. 2016. Vol. 2. Available: https://www.nature.com/articles/npjqi201621 (Nature)
2. Mannalath V., Mishra S., Pathak A. A Comprehensive Review of Quantum Random Number Generators. arXiv:2203.00261, 2022. Available: https://arxiv.org/abs/2203.00261 (arXiv)
3. Morhul D., Nariezhnii O., & Hrinenko T. Threat and adversary models for QRNG web services // Radiotekhnika. 2025. No 221. P. 31–38. https://doi.org/10.30837/rt.2025.2.221.04
4. Turan M. S. et al. Recommendation for the Entropy Sources Used for Random Bit Generation, NIST SP 800-90B (Final), 2018. DOI: 10.6028/NIST.SP.800-90B. PDF: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-90b.pdf (NIST Publications)
5. Ma X. et al. Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction // Phys. Rev. A. 2013. Vol. 87, 062327. DOI: 10.1103/PhysRevA.87.062327 (Physical Review)
6. Chouhan S. et al. FPGA-based Toeplitz Strong Extractor for Quantum Random Number Generators. arXiv:2505.02868, 2025. Available: https://arxiv.org/abs/2505.02868 (arXiv)
7. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, Aug. 2018. Available: https://datatracker.ietf.org/doc/html/rfc8446 (IETF Datatracker)
8. Temoshok D. et al. Digital Identity Guidelines: Authentication and Authenticator Management NIST SP 800-63B-4, 2025. PDF: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b-4.pdf (NIST Publications)
9. Hardt D. The OAuth 2.0 Authorization Framework // RFC 6749, Oct. 2012. Available: https://datatracker.ietf.org/doc/html/rfc6749 (IETF Datatracker)
10. Jones M., Bradley J., and Sakimura N. JSON Web Token (JWT) // RFC 7519, May 2015. Available: https://datatracker.ietf.org/doc/html/rfc7519 (IETF Datatracker)
11. Audet F. and Jennings C. Network Address Translation (NAT) Behavioral Requirements for Unicast UDP // RFC 4787, Jan. 2007. Available: https://datatracker.ietf.org/doc/html/rfc4787 (IETF Datatracker)
12. Guha S. et al. NAT Behavioral Requirements for TCP // RFC 5382, Oct. 2008. Available: https://datatracker.ietf.org/doc/html/rfc5382 (IETF Datatracker)

13. Srisuresh P. and Holdrege M. IP Network Address Translator (NAT) Terminology and Considerations // RFC 2663, Aug. 1999. Available: https://datatracker.ietf.org/doc/html/rfc2663 (IETF Datatracker)
14. Penno R. et al. Updates to NAT Behavioral Requirements // RFC 7857, Apr. 2016. Available: https://www.rfc-editor.org/rfc/rfc7857.html (RFC Editor)
15. Cao Z. et al. Source-Independent Quantum Random Number Generation // Phys. Rev. X. Vol. 6, 011020, 2016. DOI: 10.1103/PhysRevX.6.011020 (Physical Review)
16. Wang C. et al. Provably-secure quantum randomness expansion with uncharacterized measurement devices // Nature Communications, 2023. DOI: 10.1038/s41467-022-35556-z (Nature)
17. Bamps C., Massar S., Pironio S. Device-independent randomness generation with low-power states // Quantum, 2018; Pironio et al., Nature, 2010. Available: https://quantum-journal.org/papers/q-2018-08-22-86/ (quantum-journal.org) DOI:10.22331/q-2018-08-22-86
18. Joch D. et al. Certified random-number generation from quantum steering // Phys. Rev. A. Vol. 106, L050401, 2022. DOI: 10.1103/PhysRevA.106.L050401 (Physical Review)
19. Kumar A. Nai, Kumar V. Device-independent, megabit-rate quantum random number generation with live quantumness certification. arXiv:2412.18285, 2024. Available: https://arxiv.org/abs/2412.18285 (arXiv)
20. Rukhin A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST SP 800-22 Rev. 1a, 2010. PDF: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf (NIST Publications)
21. NIST, FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), 2024. Web/PDF: https://csrc.nist.gov/pubs/fips/203/final; https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf (NIST Computer Security Resource Center, NIST Publications) DOI: 10.6028/NIST.FIPS.203
22. NIST, FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA), 2024. Web/PDF: https://csrc.nist.gov/pubs/fips/204/final; https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf (NIST Computer Security Resource Center, NIST Publications) DOI:10.6028/NIST.FIPS.204
23. NIST, FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA), 2024. Web/PDF: https://csrc.nist.gov/pubs/fips/205/final; https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf (NIST Computer Security Resource Center, NIST Publications) DOI:10.6028/NIST.FIPS.205
24. NIST News, “NIST releases first 3 finalized post-quantum encryption standards,” Aug. 13, 2024. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (NIST)
25. IETF, “Best Current Practice 127: Network Address Translation (NAT) Behavioral Requirements,” comprising RFC 4787 (UDP), RFC 6888 (CGN) and RFC 7857 (Updates), 2007–2016. Available: IETF Datatracker (BCP 127 info page https://datatracker.ietf.org/doc/bcp127/).
26. Zhang X.-G., Nie Y.-Q., Zhou H., Liang H., Ma X., Zhang J., and Pan J.-W. Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction // Review of Scientific Instruments. 2016. Vol. 87, no. 7. P. 076102. DOI:10.1063/1.4958663. (Preprint: arXiv:1606.09344).
27. Scarfone K. and Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS), NIST SP 800-94, 2007. DOI:10.6028/NIST.SP.800-94
28. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev.5, 2020. DOI:10.6028/NIST.SP.800-53r5

Надійшла до редколегії 17.05.2025

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