УДК 004.056 **DOI:10.30837/rt.2025.2.221.04**

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

МОДЕЛЬ ПОРУШНИКА ТА МОДЕЛЬ ЗАГРОЗ ДЛЯ ВЕБ-СЕРВІСУ QRNG

Вступ

У сучасних інформаційних системах генерація випадкових чисел є критично важливою для забезпечення криптографічної стійкості, автентичності та цілісності даних. Квантові генератори випадкових чисел (QRNG, quantum random number generator) використовують фундаментальні принципи квантової механіки для створення істинної випадковості, яка не може бути передбачена або відтворена класичними засобами [1]. Завдяки цьому QRNG стають ключовим компонентом у побудові високонадійних криптографічних систем, особливо в контексті постквантової безпеки.

Зі зростанням популярності хмарних рішень та сервісної моделі розгортання QRNG (наприклад, через Application Programming Interface (API) або як частину сервісів "random-as-a-service") постає необхідність комплексного аналізу безпекових ризиків. Веб-сервіси QRNG, незважаючи на високу якість джерела випадковості, залишаються вразливими до традиційних та спеціалізованих кіберзагроз, зокрема атак на канал передачі, підробки API, компрометації QRNG тощо [2, 3].

Незважаючи на існування загальних підходів до моделювання загроз (наприклад, STRIDE [4]) та моделей порушників (зовнішні, внутрішні[5]), модель загроз для веб-сервісу QRNG залишається недостатньо дослідженою. Водночас компрометація такого сервісу може мати катастрофічні наслідки, особливо для систем, криптографічна стійкість яких залежить від справжньої випадковості.

Метою статті є розробка моделі загроз та моделі порушника для веб-сервісу QRNG. У роботі досліджено типові архітектури таких сервісів, визначені потенційні вектори атак та профіль порушника, обґрунтовано та надано рекомендації щодо посилення інформаційної безпеки даного класу систем.

1. Методологія моделювання

Моделювання загроз і моделювання порушника є фундаментальними етапами при розробці системи захисту для будь-якої інформаційної системи, зокрема для веб-сервісу QRNG. У даній роботі для побудови моделі загроз і моделі порушника використано комплексний підхід, що поєднує стандартизовані методики аналізу ризиків, адаптовані до специфіки архітектури QRNG.

Для моделювання загроз використано адаптовану версію методології STRIDE, що запропонована компанією Microsoft, яка дозволяє класифікувати загрози за шістьма категоріями: підміна особи (Spoofing), модифікація даних (Tampering), відмова від дій (Repudiation), розголошення інформації (Information Disclosure), відмова в обслуговуванні (Denial of Service) та підвищення привілеїв (Elevation of Privilege) [4]. Цей підхід є ефективним для виявлення типових атак на веб-сервіси, включно з API, каналами зв’язку та обробкою даних, що робить його релевантним для аналізу безпеки QRNG як сервісу.

У якості основи для класифікації ризиків використано підхід, рекомендований стандартом ISO/IEC 27005, який описує процес управління ризиками інформаційної безпеки: ідентифікація активів, оцінка загроз, вразливостей, наслідків і ймовірностей [5]. Також враховано національні вимоги до захисту інформації, що викладені у нормативному документі НД ТЗІ 1.4-001-2000, зокрема щодо категоризації активів, типів порушників та цілей атак [6].

Розробка моделі загроз виконувалася у кілька етапів:

1. Ідентифікація активів – визначення критичних компонентів QRNG-сервісу: фізичний генератор, API, обробник запитів, клієнтська сторона, канал зв’язку.

2. Ідентифікація загроз – аналіз потенційних загроз згідно з категоріями STRIDE, а також з урахуванням специфіки квантових пристроїв (наприклад, вплив на джерело випадковості).

3. Оцінка ризиків – визначення ймовірності реалізації загрози та можливого збитку для кожного активу.

4. Формалізація результатів – представлення моделі загроз у вигляді таблиці, що включає тип загрози, відповідний актив, можливий вплив і приклади реалізації.

Модель порушника базується на принципах, закладених у стандарті НД ТЗІ 1.1-002-99, де порушники класифікуються за такими ознаками [9]:

– перший рівень визначає найнижчий рівень можливостей проведення діалогу з КС і запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

У моделі враховано профілі типових порушників. Для кожного профілю визначено потенційні вектори атаки, типові загрози, які можуть бути реалізовані, та ймовірність їх успішного виконання. При формалізації архітектури системи та побудови STRIDE-матриці використовується таблиця імовірність/вплив, що наведена у розд. 4 табл.3, та діаграма потоку даних (DFD – data flow diagram), яка приведена на рис. 1. Для візуалізації взаємозв'язку між порушниками, вразливостями та наслідками атак використовуються графи атак [7]. Приклад графів атак TA01 та TA02 на QRNG веб-сервіс наведено на рис. 2.

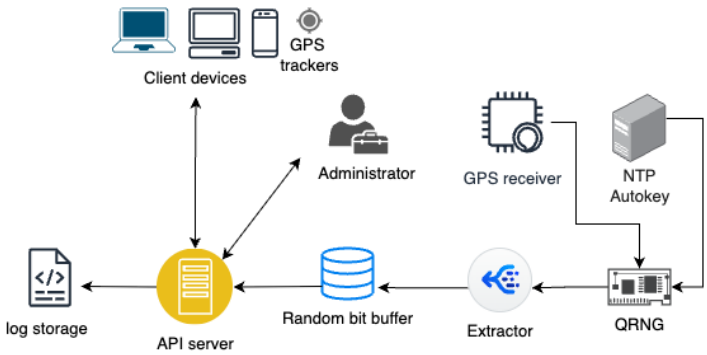

Рис. 1. Діаграма потоку даних (DFD)

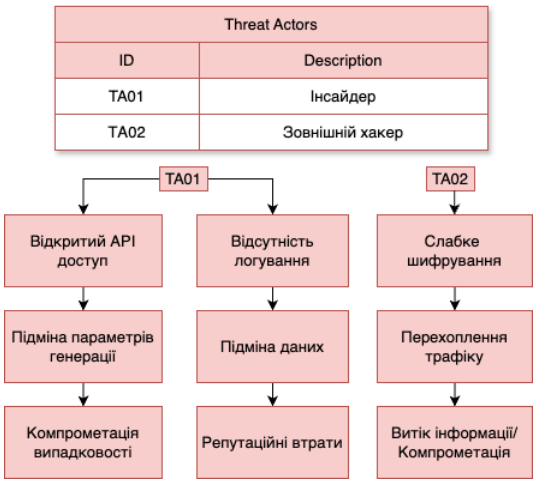

Рис. 2. Приклади графів атак на QRNG веб-сервіс

2. Розробка моделі загроз для веб-сервісу QRNG за методологією STRIDE

Модель загроз є невід'ємною складовою побудови системи захисту QRNG веб-сервісу, оскільки дозволяє ідентифікувати можливі атаки, оцінити їхній вплив та розробити відповідні контрзаходи. У контексті веб-сервісів, що забезпечують генерацію випадкових чисел, критичною є безперервність генерації, цілісність результатів та довіра до джерела випадковості [1]. Враховуючи специфіку веб-сервісу QRNG, слід звернути увагу на те, що навіть мінімальне порушення випадковості у вихідному потоці може призвести до генерації передбачуваних криптографічних ключів, що ставить під загрозу всю систему, яка базується на QRNG [3].

На основі аналізу типової архітектури QRNG-сервісу (локальний квантовий генератор, серверна частина з API, канали передачі даних, інтерфейс клієнта) було виділено такі критичні активи:

– QRNG-пристрій – джерело фізично згенерованої випадковості;
– сервер API – компонент, що обробляє запити та генерує відповіді;
– канал зв'язку (інтернет) – передача результатів до клієнта;
– буфер обробки/постобробки (екстрактор) – цифрова обробка випадкових бітів;
– логування та моніторинг – системи контролю коректності функціонування;
– інтерфейс клієнта.

Для оцінки рівня впливу загроз були використані значення, що наведені в табл. 1.

Таблиця 1

Рівень впливу загрози	Опис
1	незначний (низький)
2	нижчий за середній
3	середній
4	вищий за середній
5	значний (високий)

Із застосуванням методології STRIDE був проведений аналіз вразливості кожного активу веб-сервісу QRNG до шести класів загроз, результати аналізу наведено на рис. 3. Додатково враховано специфіку квантових пристроїв, зокрема можливість впливу на джерело генерації з боку навколишнього середовища або сторонніх сигналів.

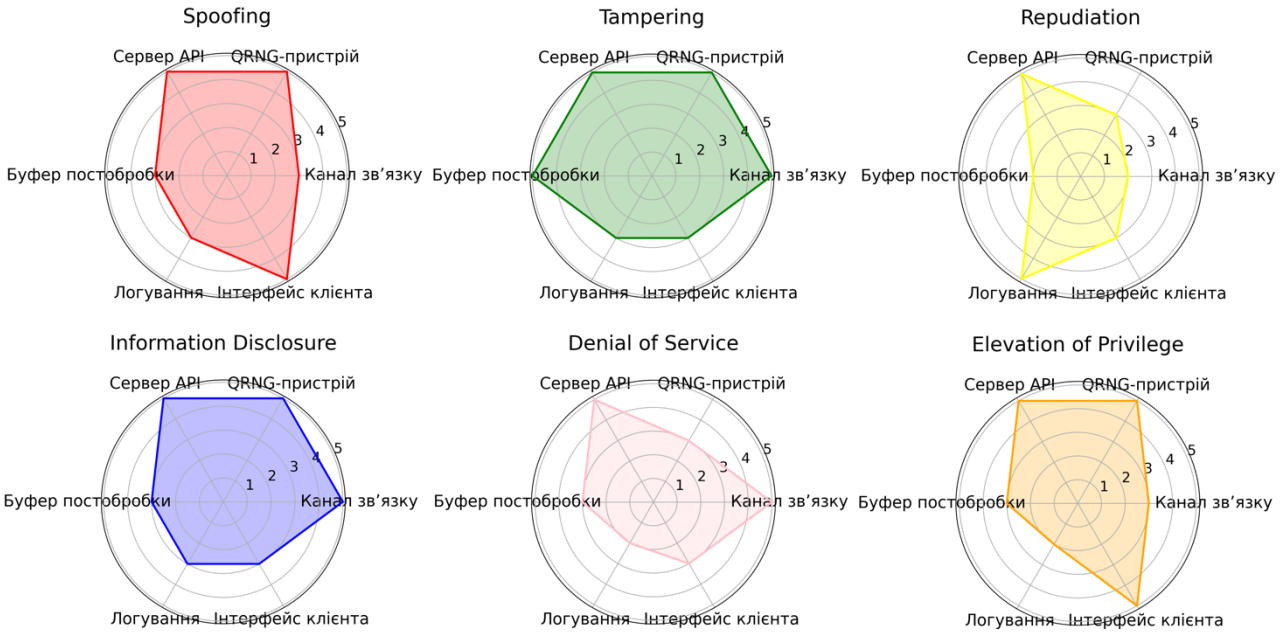

Рис. 3. Результати аналізу активів веб-сервісу QRNG згідно з методологією STRIDE

Результати аналізу показали, що найбільш вразливими елементами системи є: сервер API, QRNG пристрій та канал зв'язку, які схильні до більшої кількості загроз відносно решти активів. Для подальшої формалізації ризику застосовується матриця ймовірність/вплив, що надана у розд. 4 табл. 3.

3. Розробка моделі порушника

У процесі аналізу безпеки веб-сервісу QRNG особливу увагу слід приділити ідентифікації потенційних порушників – суб'єктів, здатних ініціювати загрози для конфіденційності, цілісності та доступності системи. Побудова моделі порушника дозволяє краще зрозуміти мотиви, можливості та технічні ресурси атакуючих сторін, що є важливим для проектування заходів захисту критичних програмних систем [8]. Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії. По відношенню до сервісу порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони) [6].

Згідно з підходами, що використовуються в національному нормативному документі НД ТЗІ 1.4-001-2000 [6], модель порушника повинна визначати:

– можливу мету порушника та її градацію за ступенями небезпечності для АС;
– категорії осіб, з числа яких може бути порушник;
– припущення про кваліфікацію порушника;
– припущення про характер його дій.

Класифікація порушників виконується за наступними критеріями [6]:

– мета;
– категорія особи;
– рівень можливостей та доступу;
– рівень обізнаності про систему;
– методи та засоби.
– місце здійснення дій.

Мету порушника визначено шляхом дослідження і класифікації вразливостей, враховуючи технічні особливості веб-сервісу QRNG:

– отримання атрибутів доступу споживачів з метою перехоплення даних та їх подальшого використання або поширення;

– маніпуляція середовищем коду екстрактора з метою подальшого впливу на процес генерації випадкових чисел під час роботи QRNG;

– компрометація криптографічних бібліотек з метою підміни джерела випадкових чисел під час виконання криптографічних операцій шляхом інтеграції менш стійкого програмного генератора випадковості;

– відновлення вихідних даних QRNG з метою подальшого їх використання або поширення;

– несанкціонований доступ до системи та її програмних або апаратних елементів з метою фізичного впливу на апаратну інфраструктуру або шпигунства;

– порушення випадковості з метою компрометації ресурсу в цілому;

– блокування роботи сервісу або зупинки передачі випадкових чисел кінцевим споживачам.

За рівнем обізнаності порушника запропоновано наступну класифікацію:

– споживачі даних, які мають інформацію про можливості сервер API;

– спеціалісти, які володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– адміністратор системи – має доступ до системи і відповідну документацію про архітектуру системи і її роботу;

– розробник системи – має повну інформацію про програмну частину системи, її вразливі місця, рівень захищеності;

– спеціаліст по QRNG приладам – володіє високим рівнем знань у галузі квантової електроніки, особливо у фізичних приладах квантових генераторів випадкових чисел.

За використовуваними методами і способами порушників запропоновано класифікувати згідно [6] як таких, що:

– використовують виключно агентурні методи одержання відомостей;

– використовують пасивні технічні засоби перехоплення інформаційних сигналів;

– використовують виключно штатні засоби системи або недоліки проєктування КСЗІ для реалізації спроб НСД;

– використовують способи і засоби активного впливу на систему, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії порушників запропоновано класифікувати як:

– з одержанням доступу до QRNG;

– з одержанням доступу до засобів адміністрування;

– без одержання доступу.

На основі цих критеріїв та особливостей веб-сервісу QRNG сформовано профіль порушника, що представлений в табл. 2.

Таблиця 2

Категорія осіб	Зовнішній (З)
	Внутрішній (ВН)
Характер дій	Навмисний (Н)
	Випадковий (ВП)
Рівень можливостей та доступу	Перший рівень (1)
	Другий рівень (2)
	Третій рівень (3)
	Четвертий рівень (4)
Рівень обізнаності про систему	Споживач даних (СД)
	Спеціаліст (СП)
	Адміністратор системи (А)
	Розробник системи (Р)
	Спеціаліст по QRNG приладам (С)
Методи та засоби	Агентурні (АГ)
	Пасивні (П)
	Штатні (Ш)
	Активні (АК)
Місце здійснення дій	З одержанням доступу до QRNG (Д)
	З одержанням доступу до засобів адміністрування (ЗА)
	Без одержання доступу (БД)
Мета дій	Отримання атрибутів доступу споживачів (АС)
	Маніпуляція середовищем коду екстрактора (МС)
	Компрометація криптографічних бібліотек (КБ)
	Відновлення вихідних даних QRNG (ВД)
	Несанкціонований доступ до системи (НСД)
	Порушення випадковості (ПВ)
	Блокування роботи сервісу (БР)

4. Аналіз результатів розробки моделі загроз та моделі порушника

На основі проведеного дослідження і розроблених моделі загроз та моделі порушника для веб-сервісу QRNG побудована таблиця імовірність/вплив для кожної загрози із врахуванням категорії загрози за моделлю STRIDE (табл. 3). Значення впливу розраховано експертним методом (рис. 3). Оцінювання ризику базується на двох ключових параметрах: ймовір-

ність реалізації та ступінь впливу. Відповідно до стандарту ISO/IEC 27005 [5], ризик розраховується як

$$,\qquad (1)$$

де R – загальний ризик, P – ймовірність реалізації загрози, C – її вплив.

Таблиця 3

Загроза	Актив	STRIDE	Ймовірність (P)	Вплив (C)
АС	сервер API інтерфейс клієнта	Spoofing	Висока	5
МС	сервер API екстрактор	Repudiation	Висока	4
КБ	QRNG екстрактор	Tampering	Середня	5
ВД	QRNG	Information Disclosure	Середня	5
НСД	QRNG сервер API канал зв'язку	Elevation of privilege	Низька	5
ПВ	QRNG екстрактор	Tampering	Низька	5
БР	канал зв'язку сервер API інтерфейс клієнта	Denial of Service	Висока	4

Враховуючи виявлені загрози і профіль порушника, розробка ефективних заходів захисту веб-сервісу QRNG вимагає інтегрованого підходу, який поєднує технічні, організаційні та процедурні механізми. Випадкові числа, згенеровані QRNG, можуть використовуватися у високозахищених криптографічних контекстах (наприклад, для генерації ключів у постквантових протоколах), і навіть незначне порушення їх цілісності може мати катастрофічні наслідки [1].

Техніки пом'якшення загроз для методології STRIDE, що запропоновані організацією OWASP, наведено у табл. 4 [10]

Таблиця 4

Тип загрози	Техніки пом'якшення загроз
Spoofing Identity	1. Відповідна автентифікація 2. Захист секретних даних 3. Не зберігати секрети
Tampering with data	1. Відповідна авторизація 2. Геші 3. MAC-коди (коди автентифікації повідомлень) 4. Цифрові підписи 5. Протоколи з захистом від підробки
Repudiation	1. Цифрові підписи 2. Мітки часу 3. Журнали аудиту
Information Disclosure	1. Авторизація 2. Протоколи з підвищеним рівнем конфіденційності 3. Шифрування 4. Захист секретів 5. Не зберігати секрети
Denial of Service	1. Відповідна автентифікація 2. Відповідна авторизація 3. Фільтрація 4. Обмеження (наприклад, швидкості запитів) 5. Якість обслуговування (QoS)
Elevation of privilege	1. Використовувати принцип найменших привілеїв

Обґрунтовано та рекомендовано наступні технічні заходи безпеки для веб-сервісу QRNG:

Захист каналу передачі даних. Передача випадкових чисел від сервера до клієнта має відбуватись виключно через захищений канал з використанням протоколів TLS 1.3 або вище. Сертифікати повинні регулярно оновлюватись, а конфігурації перевірятись на відсутність слабких шифрів [11].

Автентифікація та авторизація API. Доступ до QRNG через API повинен здійснюватися за допомогою багатофакторної автентифікації (наприклад, біометрична або OAuth 2.0 з підтримкою короткоживучих токенів) та систем контролю доступу з мінімальними привілеями [12].

Постобробка вихідних даних. Для забезпечення ентропійності та стійкості до маніпуляцій рекомендується впроваджувати процедури постобробки (наприклад, Von Neumann, Trevisan extractors), верифіковані незалежним аудитом.

Моніторинг та аудит. Усі критичні компоненти повинні логуватись, з підтримкою зовнішнього збору логів та аналізу подій. Особлива увага приділяється незвичній поведінці API, зміні патернів генерації або появі повторів у потоках.

Тестування випадковості. Регулярне застосування стандартних тестів на випадковість (наприклад, NIST SP 800-22, Dieharder) дозволяє виявити збої у роботі QRNG на ранніх етапах [13].

Обґрунтовано та рекомендовано наступні організаційні заходи безпеки для веб-сервісу QRNG:

Розмежування доступу. Адміністративний, технічний і операційний доступи до QRNG-системи повинні бути чітко розмежовані з використанням принципу найменших привілеїв.

Внутрішній контроль інсайдерів. Передбачено регулярні перевірки дій співробітників з доступом до критичної інфраструктури. Логування доступу до пристроїв і зміни конфігурацій має бути обов’язковим.

Регулярний аудит безпеки. Незалежна перевірка безпеки сервісу з боку третіх сторін не рідше одного разу на рік забезпечує відповідність актуальним вимогам кібербезпеки.

План реагування на інциденти. Має бути створено формалізований план дій у разі виявлення аномалій, включно з негайною ізоляцією сервісу, повідомленням користувачів та перезапуском QRNG з перевіркою ентропії [14].

Висновки

Проведено комплексне дослідження з метою розробки моделі загроз і моделі порушника для прототипу веб-сервісу QRNG. З огляду на критичну роль QRNG у забезпеченні криптографічної стійкості інформаційно-комунікаційних систем, захист таких сервісів має розглядатися як питання національної та корпоративної безпеки.

Проведений аналіз дозволив виявити низку специфічних загроз, характерних саме для QRNG як веб-сервісу. На відміну від традиційних PRNG (pseudorandom number generators), квантові генератори залежать від фізичних джерел ентропії, які можуть бути піддані впливу як технічного, так і середовищного характеру. Було встановлено, що навіть часткова компрометація фізичного генератора або алгоритмів обробки вихідних бітів може призвести до непередбачуваних наслідків у криптографічних протоколах, що використовують такі дані.

З використанням методології STRIDE побудовано модель загроз, яка враховує ключові активи веб-сервісу QRNG: фізичний пристрій QRNG, API, канали зв'язку, буфери обробки даних, а також логування і моніторинг. Побудовано модель порушника, яка класифікує атакуючих за рівнем доступу, обізнаністю, ресурсною базою та мотивацією.

Результати оцінки ризиків показали, що найбільшу небезпеку становлять загрози, пов’язані з перехопленням або маніпуляцією генерації випадкових чисел, а також фізичним впливом на QRNG.

Враховуючи розроблені модель порушника та модель загроз, обґрунтований та розроблений комплекс рекомендацій, що включає як технічні заходи (TLS, постобробка, аудит), так і організаційні (контроль доступу, інцидент-менеджмент, аудит безпеки) заходи безпеки.

Таким чином, розроблені модель порушника і модель загроз є уніфікованим підходом до оцінки безпеки веб-сервісу QRNG. Використання цих моделей дозволить розробникам і операторам таких сервісів ідентифікувати слабкі місця, мінімізувати ризики компрометації генерації випадкових чисел та зберегти довіру до криптографічних механізмів, що базуються на квантовій ентропії.

Список літератури:

1. M. Herrero-Collantes and J. C. Garcia-Escartin. Quantum random number generators // Rev. Mod. Phys. Marh 2017. Vol. 89, no. 1. P. 015004. DOI: 10.1103/RevModPhys.89.015004
2. T. Lunghi et al. Self-testing quantum random number generator // *Phys. Rev. Lett*. Apr. 2015. Vol. 114, no. 15. P. 150501. DOI:10.1103/PhysRevLett.114.150501
3. M. Stipčević and C. K. Koc. True random number generators // Open Problems in Mathematics and Computational Science. Springer, 2014. P. 275–315. DOI:10.1007/978-3-319-10683-0_12, link: https://cetinkayakoc.net/docs/b08.pdf
4. Microsoft Corporation. The STRIDE Threat Model // Microsoft Docs, 2005. link: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
5. ISO/IEC 27005:2022, Information technology – Security techniques – Information security risk management. International Organization for Standardization, 2022.
6. ДСТЗІ України НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Київ, 2000. link: https://tzi.com.ua/downloads/1.4-001-2000.pdf
7. B. Schneier, Attack Trees: Modeling Security Threats, Dr. Dobb's // Journal, 1999. link: https://www.schneier.com/academic/archives/1999/12/attack_trees.html
8. G. McGraw and G. Hoglund, Exploiting Software: How to Break Code, Boston, MA: Addison-Wesley, 2004. link: https://archive.org/details/Exploiting_Software_How_To_Break_Code/mode/2up
9. ДСТЗІ України НД ТЗІ 1.1-002-99. Типове положення про службу захисту інформації в автоматизованій системі. Київ, 1999. link: https://tzi.com.ua/downloads/1.1-002-99.pdf.
10. L. Conklin, V. Drake, S. Strittmatter, Z. Braiterman, A. Shostack. Threat Modeling Process // OWASP.org link: https://owasp.org/www-community/Threat_Modeling_Process#stride-threat--mitigation-techniques.
11. C. Evans, C. Palmer, and R. Sleevi. Transport Layer Security (TLS) Parameters // IETF, RFC 9325, Nov. 2022. link: https://www.rfc-editor.org/rfc/rfc9325
12. D. Hardt. The OAuth 2.0 Authorization Framework // IETF, RFC 6749, Oct. 2012. link: https://tools.ietf.org/html/rfc6749
13. L. Bassham et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications // NIST Special Publication 800-22, Rev. 1a, Apr. 2010. link: https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final
14. A. Nelson, S. Rekhi, M. Souppaya, K. Scarfone et al. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile // NIST SP 800-61 Rev. 3, Apr. 2025. link: https://csrc.nist.gov/pubs/sp/800/61/r3/final

Надійшла до редколегії 25.02.2025

Відомості про авторів:

Моргуль Дмитро Миколайович – аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, Харківський національний університет імені В. Н. Каразіна,; 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