Висновки. Мікроконтролерні системи у робототехнічних комплексах є критично важливими та водночас вразливими до широкого спектра кіберзагроз, включаючи фізичний доступ, модифікацію прошивки, перехоплення даних та атаки побічними каналами. Більшість сучасних вбудованих систем не забезпечують достатнього рівня криптографічного захисту та контролю доступу. Ефективний захист досягається шляхом комплексного підходу: апаратні механізми (TrustZone, Secure Enclave, Read-Out Protection), програмні засоби (шифрування даних, цифровий підпис прошивки, Secure Boot) та захищені комунікаційні протоколи (TLS/DTLS) з автентифікацією пристроїв. Впровадження цих методів підвищує надійність і стійкість систем до кібератак, а подальші дослідження повинні зосереджуватися на оптимізації захисту для ресурсно-обмежених мікроконтролерів, безпеку робототехнічних комплексів протягом усього життєвого циклу системи.

1. NISTIR 8259. Foundational Cybersecurity Activities for IoT Device Manufacturers. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8259.pdf
2. OWASP IoT Top 10. https://owasp.org/www-project-internet-of-things/
3. ARM TrustZone Documentation. https://developer.arm.com/documentation/ 100690/latest
4. FIPS 197: Advanced Encryption Standard (AES). https://csrc.nist.gov/publications/detail/fips/197/final
5. Secure Boot. Trusted Computing Group. https://trustedcomputinggroup.org/ resource/secure-boot/
6. RFC 6347: Datagram Transport Layer Security (DTLS). https://datatracker.ietf.org/doc/html/rfc6347

Аналіз методів тестування генераторів псевдовипадкових чисел відповідно до стандартів NIST та ISO

УДК 004.056

Олег Гарасимчук

Національний університет "Львівська політехніка", oleh.i.harasymchuk@lpnu.ua

Генератори псевдовипадкових чисел (ГПВЧ) є невід'ємним елементом сучасних інформаційних систем. Їхнє застосування охоплює значно ширший спектр завдань, ніж традиційно прийнято вважати: від застосувань для моделювання різноманітних процесів до використання в задачах кібербезпеки [1]. Якість вихідних послідовностей ГПВЧ безпосередньо визначає достовірність результатів усіх перерахованих процесів. Хоча в криптографії до ГПВЧ пред'являються найвищі вимоги (необоротність, стійкість до відновлення стану, перевірка за NIST SP 800-22), аналогічна якість випадковості є критичною і для не-криптографічних завдань, де погані ГПВЧ призводять до нерепродукованих результатів фаззингу чи помилкових висновків ML-моделей.

Попри широке практичне застосування, методологія оцінювання якості ГПВЧ у не-криптографічних контекстах залишається недостатньо

систематизованою. Більшість існуючих публікацій або орієнтовані виключно на криптографічне застосування генераторів, або обмежуються поверхневим описом окремих тестових пакетів. Разом із тим дослідники фіксують, що жодний ізольований метод тестування не здатний повністю верифікувати якість ГПВЧ: кожен з існуючих підходів має власні обмеження щодо виявлення прихованих статистичних закономірностей.

Основу нормативної бази тестування ГПВЧ формує декілька ключових міжнародних документів, які визначають методологічні вимоги та критерії оцінювання якості генераторів (таблиця 1).

Таблиця 1

Порівняльна характеристика основних стандартів тестування ГПВЧ

Стандарт	Область застосування	Ключові методи / вимоги
NIST SP 800-22 Rev.1a	Статистичне тестування послідовностей	15 статистичних тестів: frequency, runs, DFT, approximate entropy, cumulative sums та ін.
NIST SP 800-90B	Оцінювання джерел ентропії	Вимірювання мін-ентропії; IID- та non-IID-треки; валідація джерел випадковості
ISO/IEC 18031:2011	Вимоги до механізмів генерації	Загальна архітектура RBG; вимоги до сідування *(seeding)* та ресідування генераторів
ISO/IEC 20543:2019	Тестування в рамках ISO/IEC 15408 та 19790	Методи аналізу для сертифікації RBG у складі криптографічних модулів

Порівняльний аналіз методів тестування виявляє низку системних обмежень. По-перше, NIST SP 800-22 [2] розроблявся переважно для верифікації криптографічних генераторів, тому його критерії якості не повністю відповідають вимогам фаззингу чи тестування ML-систем. По-друге, тривалість виконання стандартизованих тестів (зокрема, процедур оцінювання ентропії за NIST SP 800-90B [3]) становить більше години навіть для одного джерела, що унеможливлює застосування в умовах ресурсно-обмежених IoT-пристроїв. Фахівці з безпеки вже вказують на доцільність оновлення керівних документів NIST для врахування вимог безпеки систем машинного навчання.

На основі аналізу можна виділити такі практичні рекомендації для кібербезпеки.

- Для QA-тестування і фаззингу достатньо базового пакета NIST SP 800-22 разом із TestU01 (мінімум SmallCrush). Для довгоперіодних генераторів варто додати спектральний аналіз та перевірку автокореляції.
- Для IDS/IPS та систем виявлення аномалій обов'язковою є оцінка мін-ентропії згідно з NIST SP 800-90B, оскільки саме вона визначає реальну непередбачуваність джерела.
- У тестуванні ML-систем слід доповнювати класичні статистичні методи ML-аналізом прихованих патернів, бо частина атак на ГПВЧ не виявляється стандартними тестами.

- Для IoT і вбудованих рішень доцільно використовувати полегшені набори тестів або спеціалізовані фреймворки з підтримкою паралельного виконання, щоб врахувати обмежені ресурси.
- Загалом найкращий результат дає комбінований підхід, який поєднує статистичне та ентропійне тестування, оскільки вони виявляють різні типи слабких місць генераторів.

Отже, генератори псевдовипадкових чисел є критичними не лише для криптографії, але й для багатьох інших задач кібербезпеки. Їх якість визначає надійність результатів у тестуванні, пентесті, виявленні аномалій і ML-системах. Чинні стандарти (NIST та ISO) задають базові підходи до оцінювання, але повну картину забезпечує лише поєднання статистичних, ентропійних і ML-методів. Подальші дослідження мають бути спрямовані на створення адаптивних тестів для ресурсно-обмежених систем, уточнення критеріїв якості ГПВЧ для конкретних застосувань кібербезпеки та інтеграцію методів машинного навчання у стандартизовані процедури оцінювання.

1. Марія Хомік, Олег Гарасимчук. Застосування генераторів псевдовипадкових чисел та послідовностей в кібербезпеці, методи їх побудови та оцінки якості // Захист інформації. – 2023. – Т. 25, № 3. – С. 147–159. DOI: https://doi.org/10.18372/2410-7840.25.17940.
2. NIST SP 800-22 Rev. 1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / Rukhin A., Soto J., Nechvatal J., et al. – Gaithersburg, MD: National Institute of Standards and Technology, 2010. – 127 p. – DOI: 10.6028/NIST.SP.800-22r1a.
3. NIST SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation / Bassham L. III, et al. – Gaithersburg, MD: National Institute of Standards and Technology, 2018. – 88 p. – DOI: 10.6028/NIST.SP.800-90B.

Розробка застосунку для забезпечення конфіденційності користувачів шляхом анонімізації метаданих у мультимедійних файлах

УДК 004.056.5

А.А. Гринько[1], Г.В. Шаповалов[2]

Національний університет «Одеська політехніка»
10252755@stud.op.edu.ua, shapovalov@op.edu.ua

Глобальна цифровізація та масове розповсюдження мультимедійного контенту актуалізували проблему захисту персональної інформації в інформаційному просторі. Кожен медіафайл супроводжується масивом метаданих стандартів EXIF, XMP та IPTC, які часто містять критично чутливі відомості: GPS-координати, серійні номери обладнання та часові маркери. Такі дані стають підґрунтям для деанонімізації особи та підготовки атак із використанням соціальної інженерії. Більшість загальнодоступних застосунків