КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1348
УДК 004.056

Гарасимчук Олег Ігорович
к.т.н.,доцент кафедри захисту інформації
Національний Університет "Львівська політехніка", Львів, Україна
ORCID: 0000-0002-8742-8872
oleh.i.harasymchuk@lpnu.ua

БАГАТОКРИТЕРІАЛЬНА МЕТОДИКА ВИБОРУ ГЕНЕРАТОРІВ ПУАССОНІВСЬКИХ ІМПУЛЬСНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ЗАДАЧ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. У роботі досліджено генератори псевдовипадкових імпульсних послідовностей із пуассонівським законом розподілу як засіб вирішення специфічних задач кібербезпеки та захисту інформації. Розглянуто узагальнену структурну схему ГПІП та базові класи генераторів псевдовипадкових чисел, що застосовуються для їх побудови. Обґрунтовано, що вибір генератора не може здійснюватися лише за критерієм статистичної відповідності закону Пуассона, оскільки різні сценарії застосування висувають різні вимоги до статистичних, часових, обчислювальних та криптографічних характеристик. Запропоновано багатокритеріальну методику вибору генератора, яка враховує статистичну відповідність пуассонівському процесу, швидкодію, криптографічну стійкість, період/відтворюваність та апаратну реалізованість. Для задач моделювання трафіку, синтетичного генерування подій, формування джиттера, прихованої передачі даних та автентифікації пристроїв сформовано диференційовані профілі вимог до генератора. Проведено порівняльний аналіз MAGF, LCG, LFSR, CSPRNG та фізичних джерел випадковості. Обґрунтовано, що оптимальний клас генератора визначається профілем вимог конкретного сценарію, а не існує як універсальна альтернатива. Сформульовано рекомендації щодо вибору класу генератора залежно від сценарію застосування в задачах захисту інформації.

Ключові слова: генератор псевдовипадкових імпульсних послідовностей, пуассонівський процес, багатокритеріальний вибір, кібербезпека, захист інформації, криптографічна стійкість, статистичне моделювання, приховані канали, автентифікація пристроїв.

ВСТУП

На сьогоднішній день генератори псевдовипадкових послідовностей (ГПВП) та псевдовипадкових чисел (ГПВЧ) є невід'ємними складовими систем захисту інформації [1-6]. Такі генератори використовуються при формуванні криптографічних ключів, одноразових паролів, в системах автентифікації, при маскуванні трафіку, стеганографії, моделюванні шумів та при тестуванні механізмів захисту. Загалом сучасні системи кібербезпеки та стійкість механізмів захисту інформації критично залежать від якості генерації псевдовипадкових послідовностей, а саме від статистичних властивостей, періоду повторення, передбачуваності та можливості ефективної реалізації, зокрема в програмному та апаратному виконанні. Саме тому для перевірки ефективності вихідних послідовностей даних генераторів використовують тестування їх якості за допомогою графічних та оціночних тестів [7-10].

Варто зазначити, що переважна більшість таких генераторів орієнтовані на відтворення рівномірного закону розподілу. Проте існує цілий ряд специфічних практичних задач кібербезпеки, зокрема таких як моделювання трафіку кібератак, приховані канали передачі даних, захист від атак по часових каналах, що потребують керованого відтворення нерівномірного, зокрема пуассонівського характеру потоку подій у часі, що є задачею іншого класу, при якій рівномірність вихідної послідовності не є основною метою.

Особливе місце серед таких генераторів псевдовипадкових послідовностей займають генератори, вихідні імпульсні послідовності яких формуються відповідно до пуассонівської статистичної моделі. Пуассонівська модель є характерною для широкого класу випадкових процесів і може використовуватися як математична модель або механізм формування часової структури послідовності подій. При цьому сама відповідність вихідної послідовності пуассонівському розподілу не створює фізичної унікальності пристрою та не є самостійним джерелом ентропії. У задачах, де необхідно сформувати пристрій-специфічний шаблон, пуассонівська трансформація може використовуватися лише як спосіб представлення або формування часової чи бітової структури даних, отриманих від фізично залежного

джерела, наприклад PUF або TRNG. Таким чином, джерелом фізичної унікальності або ентропії є відповідне фізичне джерело, тоді як пуассонівська модель визначає статистичну структуру сформованої послідовності. Такі генератори можуть бути виконані в програмному та апаратному виконанні, що значно розширює діапазон їх можливого застосування, зокрема для задач захисту інформації.

Пуассонівський розподіл є базовою моделлю для опису явищ, що характеризуються випадковою появою дискретних подій протягом заданого інтервалу часу [11-12]. Якщо виділити лише задачі захисту інформації, то дана модель може бути спроєктована на п’ять основних класів прикладних задач:

– моделювання трафіку кібератак для тестування систем виявлення вторгнень;

– приховані канали передачі даних, що маскують інформацію під часову структуру легітимного трафіку;

– генерування синтетичних подій для навчання й оцінки систем виявлення аномалій;

– для формування джиттера – випадкових затримок, що протидіють атакам по часових каналах;

– для формування пристрій-специфічних імпульсних або часових шаблонів на основі фізично залежних джерел, зокрема PUF або TRNG, які можуть використовуватися як додатковий чинник автентифікації пристроїв та виявлення спроб їх підміни.

Важливо зазначити, що перелічені задачі попри спільну математичну основу висувають протилежні вимоги до якості генератора. А саме, якщо мова йде про задачі моделювання та тестування (перша і третя задачі з переліку), то у цьому випадку генератор повинен виглядати правдоподібно для стороннього спостерігача чи алгоритму аналізу та забезпечувати можливість відтворення. Проте для задач захисту інформації (друга, четверта та п’ята з переліку) визначальною буде криптографічна непередбачуваність результату, яка полягає в тому, що генератор не повинен дати можливості спостерігачу жодної змоги передбачити наступне значення. Фактично тут постає складне протиріччя між статистичною правдоподібністю та криптографічною непередбачуваністю в межах однієї математичної конструкції, що формує ключову проблему вибору базового генератора для конкретного сценарію застосування.

Як правило ці дві проблеми дослідниками розглядаються ізольовано, коли роботи з моделювання мережевого трафіку та детектування атак застосовують модель пуассонівських генераторів як готовий інструмент, при цьому безпосередньо не розглядаючи властивості самих генераторів. Зокрема існуючі роботи з чисельних методів генерації випадкових величин в основному зосереджені на обчислювальній ефективності, при цьому залишаючи поза увагою ключові вимоги конкретних задач безпеки.

Генератор пуассонівських псевдовипадкових послідовностей не може бути оцінений за єдиним критерієм статистичної відповідності закону Пуассона, оскільки ефективність його використання в задачах кібербезпеки визначається сукупністю статистичних, часових, обчислювальних та криптографічних характеристик.

Отже актуальною задачею є проведення аналізу та оцінювання генераторів псевдовипадкових послідовностей з пуассонівським законом розподілу з метою визначення можливостей їх ефективного використання для підвищення якості механізмів захисту інформації. Результати такого дослідження дозволять сформулювати практичні рекомендації щодо застосування даних генераторів у задачах автентифікації, генерації ключового матеріалу, моделювання та інших напрямах кібербезпеки.

Метою даної роботи є обґрунтування вибору методу генерування псевдовипадкових послідовностей з пуассонівським законом розподілу, придатного для диференційованого застосування в задачах кібербезпеки залежно від вимог до непередбачуваності результату.

Для досягнення поставленої мети необхідно виконати наступні завдання:

– виконати аналіз методів формування псевдовипадкових імпульсних послідовностей з пуассонівським законом розподілу;

– визначити основні напрями та можливості застосування таких генераторів у широкому колі задач кібербезпеки та захисту інформації;

– сформувати систему критеріїв оцінювання їх придатності для задач кібербезпеки та захисту інформації;

– виконати порівняльне оцінювання базових генераторів;

– сформувати рекомендації, щодо вибору генератора для практичного застосування у визначених сценаріях.

Наукова новизна роботи полягає у формуванні багатокритеріального підходу до вибору базового джерела для генерації псевдовипадкових імпульсних послідовностей пуассонівського типу, який, на відміну від підходів, орієнтованих переважно на статистичну відповідність розподілу, враховує одночасно статистичну відповідність процесу, обчислювальну ефективність, криптографічну непередбачуваність, період/відтворюваність та апаратну реалізованість і дозволяє формувати різні профілі вибору залежно від сценарію застосування.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Простий пуассонівський потік – це імпульсний випадковий потік, який характеризується трьома основними властивостями: стаціонарністю, відсутністю післядії та ординарністю. Стаціонарність означає незалежність імовірнісних характеристик від моменту початку часового інтервалу, відсутність післядії – незалежність кількості подій на непересічних інтервалах, а ординарність – неможливість одночасної появи двох і більше імпульсів на нескінченно малому проміжку часу. Якщо потік задовольняє всі три властивості, то ймовірність появи рівно k імпульсів за час t буде підпорядковуватися закону Пуассона [11-12]:

$$P_k(\lambda, t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}, \quad (1)$$

де λ – середнє число імпульсів за одиницю часу (інтенсивність процесу), e – число Ейлера.

Пуассонівський процес є традиційним для застосування як базової математичної моделі потоків подій та мережевого навантаження: через один параметр λ, що визначає як середнє так і дисперсію кількості подій за інтервал часу, а властивість відсутності пам'яті робить цей процес зручним для аналітичного опрацювання, та багато років використовувалася для моделювання телефонного трафіку та потоків Інтернет-з'єднань. Водночас для сучасного мережевого трафіку його застосовність залежить від конкретного типу трафіку та досліджуваного часового масштабу.

Генератор псевдовипадкових імпульсних послідовностей (ГПІП) – це алгоритмічна або апаратно-програмна система, яка формує часову послідовність подій із заданою статистичною моделлю, що в дискретній тактованій реалізації наближає пуассонівський потік.

У роботі під ГПІП розуміється дискретна тактована реалізація пуассонівського потоку, в якій у кожному тактовому інтервалі допускається не більше однієї події, а пуассонівський характер виникає як граничне наближення біноміального процесу.

Для дискретної тактованої реалізації ГПІП міжімпульсні інтервали, виражені в кількості тактів, мають геометричний розподіл із параметром p. Експоненційний розподіл міжімпульсних інтервалів виникає як його граничне наближення при зменшенні тривалості такту $\Delta t \to 0$ за умови $p = \lambda \Delta t \to 0$. Тому при оцінюванні відповідності міжімпульсних інтервалів теоретичній моделі необхідно враховувати дискретність часової шкали: для тактованої реалізації використовувати геометричний розподіл, а експоненційний розглядати як його неперервний граничний аналог.

Узагальнену структурну схему ГПІП можна подати в наступному вигляді:

1. Генератор псевдовипадкових чисел чи бітової послідовності з рівномірним законом розподілу;
2. Регістр чи схема формування початкового значення;
3. Схема порівняння з керуючим кодом *G*;
4. Логічний елемент, який пропускає тактовий імпульс на вихід лише за виконання умови порівняння.

Ймовірність появи імпульсу на виході такого ГПІП в кожному такті приблизно дорівнює:

$$p \approx \frac{G}{M}, \quad (2)$$

де M – максимально можливе значення псевдовипадкового числа. Якщо ймовірність p_i є малою, а кількість тактів – великою, то вихідна послідовність добре апроксимує пуассонівський процес з параметром λ, який пропорційний p.

У дискретному часі кількість подій за n тактів має біноміальний розподіл:

$$N(n) \sim Bin(n, p). \quad (3)$$

Пуассонівське наближення виникає за умов:

$$n \to \infty, p \to 0, \ np \to \lambda t. \quad (4)$$

Тобто:

$$Bin(n, p) \approx Pois(\lambda t). \quad (5)$$

Перевагами таких реалізацій є можливість як програмної так і апаратної реалізації, а також відносно просте керування середньою інтенсивністю вихідного потоку шляхом зміни значення керуючого коду.

Практика показує, що як джерела псевдовипадкових чисел найчастіше використовують:

– модифіковані адитивні генератори Фібоначчі (MAGF) [13];

– генератори на основі регістрів зсуву з лінійним зворотним зв'язком (LFSR) та їх комбінації [14];

– лінійні конгруентні генератори (LCG) [15];

– криптографічно стійкі генератори (CSPRNG);

– апаратні генератори істинної випадковості (TRNG), що використовують фізичні джерела ентропії;

– фізичні функції, що не клонуються (PUF), які використовують фізично унікальні властивості пристрою для формування пристрій-специфічних відгуків;

– інші генератори з прийнятними статистичними властивостями.

ГПІП на основі модифікованих адитивних генераторів Фібоначчі базуються на класичному рекурентному співвідношенні, яке доповнене нелінійним перетворенням над результатом. У роботі [4] запропоновано конкретні модифікації адитивних генераторів Фібоначчі з покращеними статистичними характеристиками саме для потреб кібербезпеки, що підтверджує практичну реалізовність підходу, розглянутого в цій статті. Звичайні адитивні генератори Фібоначчі характеризуються високою швидкодією та здатністю формувати довгі періодичні послідовності за рахунок використання рекурентних співвідношень. Їх доволі легко реалізовувати як апаратно так і програмно, що є важливою перевагою таких генераторів. Проте рекурентна природа таких генераторів зумовлює наявність внутрішньої залежності між послідовними значеннями, що в свою чергу може негативно впливати на статистичні властивості сформованої імпульсної послідовності. А при відомій структурі такого генератора, зловмисник, маючи достатню кількість спостережних значень може відновити його внутрішній стан. Введення нелінійного елемента в MAGF ускладнює таке пряме відновлення стану, оскільки для більшості практичних модифікацій розв'язання системи лінійних рівнянь стає незастосовним, хоча про повну криптографічну стійкість тут говорити не можна.

ГПІП на основі регістрів зсуву з лінійним зворотним зв'язком забезпечують найвищу швидкодію та природну апаратну реалізованість, оскільки є типовим рішенням для вбудованих систем. Проте їх рекурентна структура забезпечує для зловмисника повне відтворення внутрішнього стану за відносно короткою ділянкою спостереження.

ГПІП на основі лінійних конгруентних генераторів характеризуються високою швидкодією та простою апаратною і програмною реалізацією. Проте для них характерною є відомий структурний недолік – вони мають граткову структуру, яка потенційно проявляється в кореляціях між кортежами послідовних значень вищого порядку.

ГПІП на основі CSPRNG, побудованих із використанням криптографічних примітивів або системних джерел ентропії, за належної реалізації забезпечують значно вищу стійкість до передбачення наступних значень порівняно з некриптографічними генераторами.

ГПІП на основі апаратних генераторів істинної випадковості (TRNG) використовують для формування послідовності фізичні джерела ентропії, завдяки чому не мають детермінованої рекурентної залежності, характерної для псевдовипадкових генераторів. Їх перевагою є висока непередбачуваність за умови належної якості джерела ентропії та коректної статистичної постобробки. Недоліками є необхідність спеціалізованої апаратної реалізації, обмежена пропускна здатність фізичного джерела та потреба в контролі якості ентропії.

PUF доцільно розглядати не як безпосередній аналог TRNG, а як окремий апаратний механізм формування пристрій-специфічних відгуків. У задачах автентифікації PUF може використовуватися для формування унікальних шаблонів або ключового матеріалу, однак його властивості необхідно оцінювати окремо від властивостей генераторів випадкових послідовностей.

Пуассонівська структура може використовуватися як форма представлення або статистичної трансформації device-specific response, сформованого PUF чи іншим фізично залежним джерелом, за умови збереження його розрізняльних властивостей. У такому випадку пуассонівський генератор не замінює PUF, а використовується як механізм формування або перетворення часової чи бітової структури пристрій-специфічного відгуку.

Порівняно з ГПВЧ з рівномірним законом розподілу для ГПІП необхідно забезпечити не лише відповідність статистичного розподілу окремих випадкових величин, а також відповідність часових інтервалів між імпульсами експоненціального розподілу. Власне дана особливість істотно ускладнює побудову та оцінювання якості генераторів пуассонівських імпульсних послідовностей.

Водночас статистична відповідність розподілу кількості подій закону Пуассона сама по собі не є достатньою умовою для підтвердження пуассонівського характеру потоку. Необхідно також перевіряти розподіл міжімпульсних інтервалів: для неперервного простого пуассонівського процесу він є експоненційним, тоді як для дискретної тактованої реалізації відповідний розподіл є геометричним. Крім

того, необхідно контролювати статистичну незалежність кількості подій на непересічних часових інтервалах.

ГППП на відміну від генераторів з рівномірним законом розподілу не так масово досліджуються науковцями, хоча останніми роками інтерес до їх дослідження зростає. Основну увагу дослідники зосереджують на способах їх побудови оптимізації параметрів та забезпечення відповідності вихідної імпульсної послідовності закону Пуассона.

Як окрему групу можна виділити дослідження, що присвячені практичному застосуванню ГППП у задачах кібербезпеки. Наприклад у [3] запропоновано модель автентифікації інформаційно-оброблювальних електронних пристроїв на основі генератора імпульсних послідовностей із пуассонівським законом розподілу. Сформовані генератором бітові шаблони відтворюють властивість фізичної унікальності пристроїв: відстані Геммінга між шаблонами одного пристрою є істотно меншими, ніж між шаблонами різних пристроїв, що підтверджує доцільність використання пуассонівських послідовностей як додаткового чинника автентифікації. J.-Y. Zeng та співавтори [16] дослідили застосування пуассонівського розподілу для підвищення ефективності виявлення малошвидкісних атак типу LDoS у мережах NB-IoT із використанням згорткової нейронної мережі. Результати цієї роботи демонструють, що моделювання статистичних характеристик мережевого трафіку за допомогою пуассонівського розподілу може бути корисним для формування ознак і розпізнавання прихованих аномалій у кіберфізичних та IoT-системах. У [17] запропоновано протокол безпеки фізичного рівня для пуассонівських каналів, призначений для протидії пасивним атакам типу «людина посередині». Автори використали випадкову природу пуассонівського каналу та дворівневу схему секретного кодування, яка забезпечує захищену передачу інформації незалежно від співвідношення характеристик легітимного каналу і каналу зловмисника; це підтверджує перспективність пуассонівських моделей для побудови інформаційно-теоретичних механізмів захисту. У [18] автори застосували узагальнену пуассонівську модель для аналізу частоти кібернападів і використали байєсівський підхід із методом Монте-Карло за ланцюгами Маркова для оцінювання параметрів моделі. Робота демонструє, що пуассонівські та узагальнені пуассонівські процеси можуть бути ефективним інструментом кількісного оцінювання кіберризиків і прогнозування інтенсивності інцидентів, хоча безпосередньо не стосується генерації псевдовипадкових послідовностей. У [19] досліджено практичну реалізацію протоколу decoy-state для квантового розподілу ключів, де кількість фотонів у слабких когерентних імпульсах описується пуассонівським розподілом. Автори показують, що пуассонівська модель є важливою для оцінювання багатофотонних імпульсів, витоку інформації та потенційних можливостей зловмисника під час реалізації QKD-систем.

Але варто відзначити, що комплексне оцінювання їх ефективності саме для широкого кола задач кібербезпеки та захисту інформації залишається недостатньо пропрацьованим. Окремі роботи в цьому напрямку більше зосереджені або на статистичних властивостях генераторів, або ж на окремих застосуваннях (як правило автентифікації). Також відсутній системний аналіз основних можливостей таких генераторів в порівнянні з класичними генераторами псевдовипадкових послідовностей за базовими критеріями, які релевантні механізмам захисту інформації.

Якщо ж розглядати сценарій детектування атак, то пуассонівська модель, навпаки, виступає як інструмент. Наприклад можна виявляти DDoS-атаки за допомогою підходу на основі моделі пуассонівського розподілу з обчислювальною складністю O(n). Такий підхід на відміну від методів машинного навчання не потребує початкового етапу навчання, оскільки достатньо побудувати одну або ж кілька пуассонівських моделей легітимного трафіку на етапі попередньої обробки, а відхилення реального трафіку за межі довірчого інтервалу буде свідчити про потенційну атаку.

Пуассонівський розподіл також може використовуватися як один з можливих варіантів генерування фонового трафіку в симуляційних дослідженням SDN-мереж [20] поряд з рівномірним, гамма та експоненційним розподілами.

Для прихованих часових каналів [21] дослідження підтверджують, що як ключового аспекту для них можна виділити пошук порогового значення затримки пакета, що дасть змогу відрізнити достовірно прихований трафік від легітимного. Тут можна зазначити, що даний поріг приблизно вдвічі перевищує середнє значення міжінтервального часу легітимного трафіку. Щоб детектувати такі канали використовують тести форми розподілу (зокрема критерій Колмогорова-Смірнова), а також ентропійні тести та тести регулярності. Для прихованих часових каналів криптографічна непередбачуваність не може розглядатися ізольовано від статистичної подібності до легітимного потоку. Надмірно сильне відхилення від статистичної моделі фонового трафіку може, навпаки, підвищити виявлюваність прихованого каналу. Тому вибір генератора в цьому сценарії являє собою компроміс між криптографічною непередбачуваністю (К3) та статистичною відповідністю моделі фонового трафіку (К1).

Також варто згадати джиттер – як засіб захисту від атак по часових каналах [22]. Вставка випадкових затримок є типовим контрзаходом проти атак часового та енергетичного аналізу, хоча також методи розпізнавання образів на основі прихованих Марківських моделей [23] здатні ефективно усувати такі випадкові затримки з енергетичних слідів, що може ставити під сумнів абсолютну ефективність даного контрзаходу для малих вбудованих пристроїв. Для формування захисного джиттера перевагу доцільно надавати CSPRNG або апаратному джерелу випадковості. MAGF може розглядатися як компромісний варіант для сценаріїв, у яких вимоги до криптографічної непередбачуваності не є критичними.

Якщо ж мова йде про генерування тестових даних, то тут варто відзначити сучасну проблему нестачі розмічених даних для навчання систем виявлення аномалій, яка полягає в тому, що кількість наборів даних про події безпеки є обмеженою через питання конфіденційності та доступності, а існуючі публічні набори є часто обмежені за різноманітністю подій та кількістю міток.

Підсумовуючи, можна зробити висновок, що дослідження пуассонівських моделей у задачах кібербезпеки є зосередженими або ж на застосуванні готової моделі до конкретної задачі, або ж на суто чисельних методах генерування без визначеної прив’язки до вимог безпеки під час конкретного застосування.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз розглянутих вище задач показує, що вибір генератора неможливо звести до єдиного критерію, який би давав відповідь, про те наскільки добре відтворюється закон Пуассона. Одна й та сама пуассонівська статистична поведінка на виході не означає однакової придатності генераторів для задач кібербезпеки, оскільки після однакового статистичного перетворення можуть зберігатися принципово різні властивості базового джерела щодо передбачуваності, відновлення стану, швидкодії та апаратної реалізації. Тут варто застосувати багатовимірну методику оцінювання.

При цьому критерії оцінювання мають відображати не лише властивості сформованої імпульсної послідовності, а й характеристики базового генератора, які визначають її придатність до конкретного сценарію застосування. Це особливо важливо для задач захисту інформації, де статистично прийнятна послідовність може бути непридатною через низьку непередбачуваність, можливість відновлення внутрішнього стану або надмірні обчислювальні витрати. Тому запропонована система критеріїв повинна забезпечувати одночасне врахування статистичних, обчислювальних, криптографічних та апаратних властивостей генератора:

К1. *Статистична відповідність пуассонівському процесу* – це ступінь узгодженості вихідної імпульсної послідовності з властивостями простого пуассонівського процесу. Оцінювання К1 доцільно проводити за сукупністю статистичних показників і критеріїв, оскільки жоден окремий статистичний тест не є достатнім для підтвердження пуассонівського характеру потоку. До основних показників доцільно віднести: відповідність розподілу кількості подій закону Пуассона за критерієм χ^2; відповідність розподілу міжімпульсних інтервалів теоретичному розподілу за критерієм Колмогорова–Смірнова (KS) або іншим відповідним критерієм; співвідношення математичного очікування та дисперсії кількості подій, зокрема через показник дисперсії (dispersion index); оцінювання автокореляційних властивостей послідовності; а також перевірку статистичної незалежності кількості подій на непересічних часових інтервалах. Для дискретної тактованої реалізації міжімпульсних інтервалів використовується геометричний розподіл, тоді як експоненціальний розподіл розглядається як його неперервний граничний аналог.

К2. *Обчислювальна складність/швидкодія* – це витрати часу чи апаратних ресурсів на генерування одного значення, включно із залежністю цих витрат від параметра інтенсивності λ. У подальшому критерій К2 трактується як максимізаційний: вище значення відповідає кращій швидкодії генератора.

К3. *Криптографічна стійкість базового джерела* – це можливість відновлення внутрішнього стану генератора (а значить і передбачення майбутніх значень) за спостереженням частини послідовності на виході генератора, можливість використання як джерела ентропії або компонента генерування ключового матеріалу. Статистичне тестування вихідної послідовності не розглядається як достатня умова криптографічної стійкості генератора. Криптографічна оцінка повинна ґрунтуватися насамперед на властивостях алгоритму, ентропії початкового стану, можливості відновлення стану та передбачення наступних значень.

К4. *Періодичність та відтворюваність* – це максимальна довжина неповторюваної послідовності, яку здатен видати такий генератор до її циклічного повторення. Для задач моделювання висока відтворюваність є позитивною властивістю, тоді як у задачах безпеки необхідність прихованого стану та непередбачуваність можуть мати пріоритет над детермінованою відтворюваністю.

К5. *Апаратна реалізованість* – це придатність методу, що використовується до ефективної реалізації у вбудованих системах, що є особливо актуальним для задач автентифікації пристроїв на основі фізичної унікальності. При цьому потрібно враховувати обсяг необхідних обчислювальних ресурсів, можливість реалізації на FPGA та мікроконтролерах.

Для підвищення обґрунтованості багатокритеріального вибору доцільно здійснювати декомпозицію узагальнених критеріїв $K_1 - K_5$на сукупність підкритеріїв. Такий підхід дає змогу уникнути надмірного узагальнення окремих характеристик, насамперед статистичної відповідності та криптографічної стійкості, і забезпечує більш детальне врахування вимог конкретного сценарію застосування.

Критерій K_1 – статистична відповідність пуассонівському процесу доцільно представити такими підкритеріями:

– $K_{1.1}$ – відповідність розподілу кількості подій за часовий інтервал теоретичному закону Пуассона;

– $K_{1.2}$ – відповідність розподілу міжімпульсних інтервалів теоретичному розподілу: геометричному для дискретної тактованої реалізації або експоненціальному для неперервної моделі;

– $K_{1.3}$ – статистична незалежність кількості подій на непересічних часових інтервалах;

– $K_{1.4}$ – стабільність оціненого параметра інтенсивності λу часі та за різних умов формування послідовності.

Критерій K_2 – продуктивність доцільно декомпозувати на:

– $K_{2.1}$– швидкість генерації імпульсів або псевдовипадкових значень;

– $K_{2.2}$– обчислювальні та апаратні ресурси, необхідні для реалізації генератора;

– $K_{2.3}$– залежність продуктивності та ресурсних витрат від заданої інтенсивності λ.

Критерій K_3 – криптографічна стійкість базового джерела доцільно оцінювати за такими підкритеріями:

– $K_{3.1}$– ентропія та якість початкового стану (seed);

– $K_{3.2}$– складність або практична неможливість відновлення внутрішнього стану за доступною зловмиснику вихідною послідовністю;

– $K_{3.3}$– стійкість до передбачення наступних значень за відомими або частково відомими попередніми значеннями;

– $K_{3.4}$– стійкість генератора після компрометації внутрішнього стану, зокрема здатність запобігати відновленню попередніх або майбутніх значень залежно від архітектури генератора.

Критерій K_4 – періодичність та контрольованість відтворення доцільно представити такими підкритеріями:

– $K_{4.1}$– довжина періоду генератора;

– $K_{4.2}$– можливість детермінованого відтворення послідовності за заданим початковим станом;

– $K_{4.3}$– можливість керування параметрами вихідного потоку, зокрема зміною інтенсивності λ.

Критерій K_5 – апаратна реалізованість доцільно оцінювати за:

– $K_{5.1}$– придатністю до реалізації на FPGA та інших програмованих логічних пристроях;

– $K_{5.2}$– придатністю до реалізації на мікроконтролерах та вбудованих обчислювальних платформах;

– $K_{5.3}$– вимогами до обсягу пам’яті та логічних/обчислювальних ресурсів;

– $K_{5.4}$– енергоспоживанням реалізації для вбудованих та автономних пристроїв.

Таким чином, запропонована система має дворівневу структуру: на верхньому рівні використовуються п’ять агрегованих критеріїв $K_1 - K_5$, а на нижньому – їхні підкритерії $K_{i.l}$. Це дає змогу зберегти компактність інтегральної моделі оцінювання та водночас забезпечити деталізований аналіз характеристик генераторів.

Важливо зазначити, що вага цих критеріїв буде не однаковою для різних задач. Наприклад, якщо ми розглядатимемо моделювання трафіку атак, то визначальними можна вважати критерії К1 та К2, а К3 при цьому практично не матиме значення. Якщо ж мова буде йти про приховані канали, то визначальним буде саме критерій К3, а К2 вже буде другорядним.

Для систематизації запропонованого підходу на рис. 1 наведено узагальнену послідовність етапів багатокритеріальної методики вибору базового генератора для формування ГПІП.

Як видно з даного рисунку, вибір генератора здійснюється не безпосередньо за його класом, а послідовно через визначення вимог конкретного сценарію, формування системи критеріїв та їх ваг, оцінювання альтернатив, нормування отриманих показників, розрахунок інтегральної оцінки та перевірку стійкості рішення за допомогою аналізу чутливості.

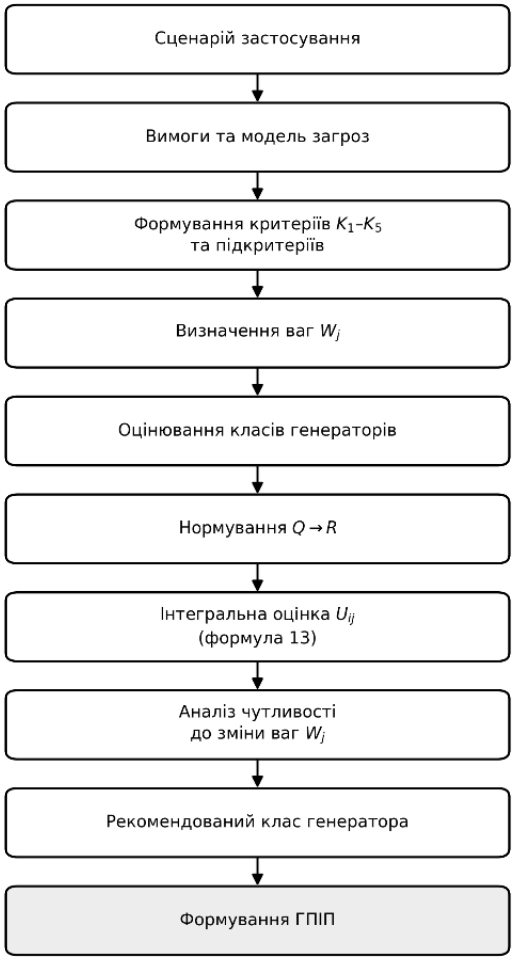

Рис. 1. Узагальнена схема багатокритеріальної методики вибору генератора псевдовипадкових імпульсних послідовностей пуассонівського типу

Формалізація задачі вибору
Нехай задано множину альтернатив:

$$G = \{G_1, G_2, \dots, G_m\}, \tag{6}$$

де G_i – клас базового генератора.
Множина критеріїв:

$$K = \{K_1, K_2, K_3, K_4, K_5\}. \tag{7}$$

Для кожного генератора формується матриця оцінювання:

$$Q = [q_{ik}], i = 1, \dots, m, k = 1, \dots, 5. \tag{8}$$

Оскільки критерії мають різні одиниці вимірювання, їх необхідно нормувати.
Для критеріїв, де більше означає краще:

$$r_{ik} = \frac{q_{ik} - q_k^{min}}{q_k^{max} - q_k^{min}}. \tag{9}$$

Для критеріїв, де менше означає краще:

$$r_{ik} = \frac{q_k^{max} - q_{ik}}{q_k^{max} - q_k^{min}}. \quad (10)$$

Тоді для сценарію S_j вводиться вектор ваг:

$$W_j = (w_{j1}, w_{j2}, \dots, w_{j5}), \quad (11)$$

причому:

$$\sum_{k=1}^{5} w_{jk} = 1. \quad (12)$$

Інтегральна оцінка:

$$U_{ij} = \sum_{k=1}^{5} w_{jk}\, r_{ik}. \quad (13)$$

Генератор із найбільшим значенням U_{ij} вважається найбільш придатним для відповідного сценарію.

Запропонований інтегральний критерій відповідає методу простого адитивного зважування (Simple Additive Weighting, SAW), що передбачає адитивність та компенсаторність критеріїв. Тому недостатньо високе значення одного критерію потенційно може компенсуватися вищими значеннями інших, а результат оцінювання залежить від обраних вагових коефіцієнтів і коректності нормування. Для задач захисту інформації така компенсаторність не завжди є прийнятною, оскільки окремі характеристики можуть мати характер обов'язкових вимог. Наприклад, критично низька криптографічна непередбачуваність не повинна компенсуватися високою швидкодією або апаратною реалізованістю.

Тому запропонована методика передбачає дворівневу процедуру вибору: на першому етапі здійснюється перевірка альтернатив на відповідність обов'язковим пороговим вимогам, а на другому – багатокритеріальне ранжування альтернатив, що пройшли таку перевірку.

Нехай для сценарію S_jзадано множину обов'язкових порогових вимог H_j. Для кожного обов'язкового критерію K_kвстановлюється мінімально допустиме нормоване значення h_{jk}. Тоді множина допустимих альтернатив визначається як:

$$G_j^* = \{G_i \in G : r_{ik} \geq h_{jk}, k \in H_j\} \quad (14)$$

Такий підхід дає змогу розділити обов'язкові вимоги безпеки та критерії оптимізації. Зокрема, для security-critical сценаріїв може бути встановлено мінімально допустимий рівень криптографічної стійкості K_3, після чого серед альтернатив, що задовольняють цю вимогу, здійснюється вибір з урахуванням швидкодії, статистичної відповідності, керованості та апаратної реалізованості.

Приклад вагового профілю сценарію може мати наступний вигляд:

Таблиця 1

Приклад вагового профілю сценарію

Сценарій	К1	К2	К3	К4	К5
Моделювання атак	0.35	0.30	0.05	0.20	0.10
Синтетичні IDS-події	0.35	0.20	0.10	0.25	0.10
Приховані канали	0.15	0.10	0.50	0.10	0.15
Джиттер	0.15	0.20	0.40	0.05	0.20
Автентифікація	0.15	0.10	0.40	0.10	0.25

Наведені в табл. 1 вагові коефіцієнти мають демонстраційний характер і використовуються для ілюстрації запропонованої методики. У практичній реалізації їх значення мають визначатися на основі експертного оцінювання, AHP або іншого формалізованого методу. Тому варто зазначити, що в конкретній практичній реалізації вагові коефіцієнти визначаються експертним опитуванням, методом аналізу ієрархій (AHP), ентропійним методом або іншим методом визначення ваг.

Таблиця 2

Якісна характеристика класів базових генераторів для побудови ГПВП

Тип генератора	К1 (статист. відповідність)	К2 (швидкодія/ продуктивність)	К3 (крипто стійкість)	К4 (період контрольованість відтворення)	К5 (апаратна реалізованість)
MAGF-базований	Висока (кращі показники багатовимірної рівномірності, ніж у LCG)	Висока (без операції множення)	Середня (пряме лінійне відновлення ускладнене нелінійним елементом; повна криптостійкість не гарантована)	Висока (суттєво довший за LCG при вдалих параметрах)	Висока
LCG-базований	Висока за прямими тестами узгодженості; потребує тестів вищого порядку для повної перевірки	Висока	Низька	Середня (обмежена модулем)	Висока
LFSR-базований	Висока	Найвища	Низька (вразливий до Берлекампа-Мессі)	Висока (2^n-1 для n-бітного регістра)	Найвища
CSPRNG-базований	Висока	Середня (нижча за LCG/LFSR)	Висока	Дуже висока	Середня
TRNG (фізичне джерело ентропії)	Залежить від якості фізичного джерела та постобробки	Низька/ середня	Висока за умови достатньої ентропії та належного контролю	Практично необмежена	Середня/ висока, залежно від реалізації

Оцінки К1–К5 не є результатами експериментального тестування конкретних реалізацій; вони сформовані як узагальнені експертні оцінки класів генераторів на основі властивостей відповідних алгоритмічних конструкцій та наведених літературних джерел.

Критерій К1 характеризує не базовий генератор безпосередньо, а статистичні властивості сформованої на його основі імпульсної послідовності за однакової схеми пуассонівського перетворення.

Для подальшого розрахунку інтегральних оцінок якісні характеристики з табл. 2 переведено в числові значення за лінійною шкалою: «Висока» / «Найвища» = 0,9; «Середня» = 0,55; «Низька» = 0,25.

Якщо експертне опитування не проводиться, квантифікацію якісних оцінок у демонстраційному прикладі можна виконати за шкалою, наведеною в табл. 3.

Таблиця 3.

Пряме шкалювання (Direct Rating / Linear Scale)

Якісна оцінка	Числове значення (шкала 0–1)	Альтернатива (шкала 0–10)
Висока / Найвища	0.90 (або 0.85–1.00)	9
Середня	0.55 (або 0.50–0.60)	5–6
Низька	0.25 (або 0.15–0.30)	2–3

Такий підхід є поширеним у методах багатокритеріального аналізу (зокрема SAW) і забезпечує можливість подальшого нормування та зваженого агрегування оцінок. У даній роботі всі критерії К1–К5 трактуються як максимізаційні (вище значення відповідає кращій характеристиці генератора). Після квантифікації якісних оцінок («Висока» = 0,9; «Середня» = 0,55; «Низька» = 0,25) матриця оцінок уже

належить інтервалу [0; 1], тому додаткова min-max нормалізація може не застосовуватися, або застосовується за формулою (9) для уніфікації шкал. Для критерію К2 (швидкодія) вище значення також означає кращий результат.

Зіставлення критеріїв К1-К5 із вимогами п'яти розглянутих прикладних класів задач захисту інформації розглянутих у вступі дає змогу сформулювати наступні практичні рекомендації (Таблиця 4). При цьому для задач автентифікації пристроїв за фізичною унікальністю PUF доцільно розглядати як окремий клас фізично обумовлених механізмів формування пристрій-специфічних відгуків, а не як різновид TRNG. Відповідно, PUF не розглядається як безпосередня альтернатива генераторам псевдовипадкових послідовностей, а використовується як окремий апаратний механізм, властивості якого можуть доповнювати властивості генератора випадкових або псевдовипадкових послідовностей.

Таблиця 4.

Рекомендації щодо вибору генератора залежно від сценарію застосування

Сценарій застосування	Визначальні критерії	Рекомендований клас генератора/механізму
Моделювання трафіку кібератак	К1, К2	LCG- або MAGF-базований генератор як доцільні варіанти
Приховані канали / стеганографія	К3	CSPRNG-базований; MAGF – прийнятний компроміс, якщо повна криптостійкість не обов'язкова, а важлива швидкодія
Синтетичні події для SIEM/IDS	К1, К4	LCG- або MAGF-базований генератор (за потреби відтворюваності – з фіксованим початковим станом)
Джиттер проти timing-атак	К3, К5	CSPRNG-базований або TRNG; MAGF – компромісний варіант за некритичних вимог до непередбачуваності
Автентифікація пристроїв за фізичною унікальністю	К3, К5	PUF; TRNG – як додаткове джерело випадковості

Такий підхід дає змогу обґрунтовано підбирати клас генератора під конкретну задачу захисту інформації, не покладаючись на єдиний «універсально найкращий» варіант.

Оскільки результати багатокритеріального вибору залежать від прийнятих вагових коефіцієнтів, доцільно також оцінювати стійкість отриманого рейтингу до їх зміни. Такий аналіз дає змогу визначити, наскільки зміна пріоритетів окремих критеріїв впливає на вибір оптимального класу генератора та чи зберігається отримане рішення за різних профілів вимог. Зокрема, для сценаріїв, у яких суттєве значення має криптографічна непередбачуваність, може оцінюватися зміна ваги критерію К3 у заданому діапазоні з визначенням граничних значень, за яких змінюється порядок переваги альтернатив. Аналогічно може оцінюватися чутливість результату до зміни ваги критерію К2, що характеризує швидкодію та обчислювальну ефективність. При цьому наведені в табл. 1 вагові профілі мають ілюстративний характер і не розглядаються як результати експертного оцінювання; їх конкретні значення мають визначатися відповідно до вимог практичної задачі та обраного методу формування ваг.

За результатами проведеного аналізу та порівняльного оцінювання можна сформувати такі рекомендації:

1. Автентифікація пристроїв. Для формування пристрій-специфічних бітових шаблонів доцільно розглядати PUF як окремий апаратний механізм, що використовує фізичні відмінності між пристроями. TRNG при цьому може застосовуватися як додаткове джерело випадковості або ентропії. Результати проаналізованих досліджень свідчать про перспективність використання фізично обумовлених властивостей пристроїв для підвищення достовірності їх автентифікації.

2. Моделювання та тестування. Рекомендується застосовувати ГПІП для імітаційного моделювання потоків подій (мережевий трафік, помилки передачі, виникнення інцидентів тощо) під час тестування систем виявлення вторгнень, систем моніторингу та оцінки ефективності захисних механізмів.

3. Гібридні схеми генерації. У задачах генерування ключового матеріалу ГПІП рекомендовано використовувати не як самостійного криптографічно стійкого генератора, а як компоненту гібридних схем у поєднанні з криптографічно стійкими генераторами або ж фізичними джерелами ентропії.

4. Стеганографія та маскування. ГПІП можуть бути застосовані для формування маскуючих послідовностей та керування параметрами вбудовування прихованої інформації в тих випадках, коли пуассонівський характер розподілу буде ускладнювати статистичний аналіз зловмисником.

5. Проєктування та реалізація. При проєктуванні ГПІП рекомендовано обирати клас базового генератора відповідно до результатів багатокритеріального оцінювання та вимог конкретного сценарію. Для некритичних щодо криптографічної непередбачуваності задач можуть розглядатися високопродуктивні генератори, зокрема MAGF, LCG або LFSR, тоді як для задач, що висувають підвищені вимоги до непередбачуваності, доцільно застосовувати CSPRNG або фізичні джерела ентропії. При цьому обов'язково потрібно здійснювати комплексну перевірку відповідності сформованої послідовності властивостям пуассонівського процесу за сукупністю статистичних критеріїв, зокрема із застосуванням критерію χ^2 для перевірки розподілу кількості подій, критерію Колмогорова–Смірнова для оцінювання розподілу міжімпульсних інтервалів, аналізу показника дисперсії, автокореляційного аналізу та перевірки статистичної незалежності подій на непересічних часових інтервалах.

6. Обмеження застосування. Не варто використовувати ГПІП як єдине джерело випадковості в протоколах, які вимагають доведеної криптографічної стійкості при цьому не проводячи додаткове посилення (криптографічного пост-оброблення або ж комбінування з CSPRNG).

Для запропонованого багатокритеріального підходу характерними є ряд обмежень, які варто враховувати під час його практичного застосування:

– По-перше, результати оцінювання залежать від способу квантифікації якісних характеристик генераторів. Використання шкали «висока – середня – низька» дає змогу сформувати узагальнену порівняльну оцінку, проте не замінює експериментального вимірювання конкретних характеристик генератора. Саме тому наведені в табл. 2–3 значення варто розглядати як орієнтовні, а для практичного вибору доцільно використовувати результати випробувань конкретних реалізацій.

– По-друге, вагові коефіцієнти критеріїв залежать від сценарію застосування та можуть містити суб’єктивну складову, якщо визначаються експертним методом. Саме тому наведені в табл. 1 вагові профілі мають ілюстративний характер і не можуть розглядатися як універсальні для всіх практичних задач. Для підвищення обґрунтованості вибору доцільно застосовувати формалізовані методи визначення ваг, зокрема AHP, ентропійний метод або аналіз чутливості отриманого рейтингу до зміни вагових коефіцієнтів.

– По-третє, статистична відповідність сформованої послідовності пуассонівській моделі не є достатньою умовою для забезпечення криптографічної стійкості. Генератор може демонструвати високу відповідність статистичним характеристикам пуассонівського процесу, але залишатися передбачуваним за наявності відомої структури алгоритму, недостатньої довжини внутрішнього стану або слабкого механізму ініціалізації.

– По-четверте, порівняння класів генераторів не може повністю замінити аналіз конкретної реалізації. Криптографічні та статистичні властивості генератора залежать не лише від обраного класу, а й від розміру внутрішнього стану, способу ініціалізації, джерела початкового значення, параметрів рекурентного співвідношення, способу постобробки та моделі противника. Тому наведені рекомендації слід розглядати як рекомендації щодо вибору класу базового генератора, а не як твердження про безумовну перевагу одного класу над іншим.

Запропонована методика не замінює процедур криптографічної валідації генераторів, визначених відповідними стандартами та рекомендаціями, а використовується на етапі попереднього вибору архітектури залежно від прикладного сценарію.

Отже, запропонована методика є інструментом попереднього багатокритеріального вибору, який має доповнюватися експериментальним дослідженням конкретної реалізації генератора, статистичним тестуванням вихідної послідовності, оцінюванням швидкодії та, для задач захисту інформації, аналізом можливості передбачення виходу за заданої моделі противника.

Запропоновані рекомендації створюють основу для обґрунтованого вибору класу генератора відповідно до вимог конкретного механізму захисту інформації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті проведено порівняльний аналіз та обґрунтовано підхід до вибору генераторів псевдовипадкових імпульсних послідовностей з пуассонівським законом розподілу для задач кібербезпеки та захисту інформації. Розглянуто п’ять класів джерел для формування ГПІП (MAGF, LFSR, LCG, CSPRNG, апаратні генератори істинної випадковості (TRNG), що використовують фізичні джерела ентропії) та запропоновано багатовимірну методику їх оцінювання за п'ятьма критеріями – статистична відповідність закону Пуассона, обчислювальна складність, криптографічна стійкість базового джерела,

довжина періоду та апаратна реалізовність. PUF розглядається окремо як фізично обумовлений механізм автентифікації.

Показано, що вага цих критеріїв істотно залежить від класу прикладної задачі: для задач моделювання й тестування (моделювання трафіку атак, генерування синтетичних подій для SIEM) визначальними є статистична відповідність і швидкодія, тоді як для задач захисту (зокрема прихованих каналів, автентифікації і формування джиттера) зростає значущість криптографічної непередбачуваності базового джерела, однак її вагомість визначається конкретною моделлю загроз і вимогами сценарію. На основі цього зіставлення сформульовано практичні рекомендації щодо вибору класу генератора для п'яти характерних сценаріїв застосування в задачах захисту інформації, а також загальні рекомендації щодо проєктування ГППП – зокрема вибір конкретного класу базового генератора за результатами багатокритеріального оцінювання та формування комбінованих схем відповідно до вимог конкретного сценарію, із комплексною перевіркою відповідності властивостям пуассонівського процесу, що включає перевірку розподілу кількості подій, розподілу міжімпульсних інтервалів, дисперсійних характеристик, автокореляційних властивостей та статистичної незалежності подій на непересічних часових інтервалах.

Практична цінність отриманих результатів полягає у формуванні обґрунтованої методики вибору класу генератора під конкретну задачу захисту інформації замість орієнтації на єдиний «універсально найкращий» варіант.

Напрями подальших досліджень включають розробку та експериментальну апробацію конкретних алгоритмів генерації на основі узагальнених у цій статті принципів, кількісне порівняння конкретних реалізацій розглянутих класів за результатами обчислювального експерименту, дослідження чутливості отриманих рейтингів до зміни вагових коефіцієнтів, а також дослідження гібридних схем поєднання різних класів генераторів із криптографічно стійкими генераторами та фізичними джерелами ентропії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Orúe, A. B., Hernández Encinas, L., Fernández, V., & Montoya, F. (2018). A review of cryptographically secure PRNGs in constrained devices for the IoT. In H. Pérez García, J. Alfonso-Cendón, L. Sánchez González, H. Quintián, & E. Corchado (Eds.), *International Joint Conference SOCO'17-CISIS'17-ICEUTE'17* (Advances in Intelligent Systems and Computing, Vol. 649). Springer. https://doi.org/10.1007/978-3-319-67180-2_65
2. Maksymovych, V., Shabatura, M., Harasymchuk, O., Shevchuk, R., Sawicki, P., & Zajac, T. (2022). Combined pseudo-random sequence generator for cybersecurity. *Sensors, 22*, 9700. https://doi.org/10.3390/s22249700
3. Maksymovych, V., Nyemkova, E., Justice, C., Shabatura, M., Harasymchuk, O., Lakh, Y., & Rusynko, M. (2022). Simulation of authentication in information-processing electronic devices based on Poisson pulse sequence generators. *Electronics, 11*, 2039. https://doi.org/10.3390/electronics11132039
4. Maksymovych, V., Shabatura, M., Harasymchuk, O., Karpinski, M., Jancarczyk, D., & Sawicki, P. (2022). Development of additive Fibonacci generators with improved characteristics for cybersecurity needs. *Applied Sciences, 12*, 1519. https://doi.org/10.3390/app12031519
5. Almaraz Luengo, E. (2022). A brief and understandable guide to pseudo-random number generators and specific models for security. *Statistics Surveys, 16*, 137–181.
6. Khomik, M. A., & Harasymchuk, O. I. (2024). Analysis of threats to pseudorandom number and pseudorandom sequence generators and protection measures. *Ukrainian Information Security Research Journal, 25*(4), 172–184. https://doi.org/10.18372/2410-7840.25.18222
7. Khomik, M., & Harasymchuk, O. (2023). Application of pseudorandom number and sequence generators in cybersecurity, methods of their construction and quality assessment. *Ukrainian Information Security Research Journal, 25*(3), 147–159. https://doi.org/10.18372/2410-7840.25.17940
8. Popereshniak, S. V. (2022). Methodology for statistical analysis of the randomness of sequences generated by random and pseudorandom number generators. *Telecommunication and Information Technologies, 3*(76).
9. Alani, M. M. (2010). Testing randomness in ciphertext of block-ciphers using DieHard tests. *International Journal of Computer Science and Network Security (IJCSNS), 10*(4), 53–57.
10. National Institute of Standards and Technology. (2010). *A statistical test suite for random and pseudorandom number generators for cryptographic applications* (NIST Special Publication 800-22 Rev. 1a). NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf
11. Harremoës, P. (2001). Poisson's law and information theory. In *Proceedings of the 2001 IEEE International Symposium on Information Theory* (p. 46). IEEE. https://doi.org/10.1109/ISIT.2001.935909

12. Bidiuk, P. I., Tkach, B. P., & Harrington, T. (2018). *Mathematical statistics: Textbook*. Publishing House "Personal".
13. Orúe, A. B., Montoya, F., & Hernández Encinas, L. (2010). Trifork, a new pseudorandom number generator based on lagged Fibonacci maps. *Journal of Computer Science and Engineering*, *2*(2), 46–51.
14. Durga, R. S., Rashmika, C. K., Madhumitha, O. N. V., Suvetha, D. G., Tanmai, B., & Mohankumar, N. (2020). Design and synthesis of LFSR based random number generator. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 438–442). IEEE. https://doi.org/10.1109/ICSSIT48917.2020.9214240
15. Tarigan, J. T., Salim, A. C., Nababan, A. M., & Wijaya, B. (2024). Crafting the chance: Linear congruential generator in randomization system in RPGs. In *2024 International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. 270–275). IEEE. https://doi.org/10.1109/ICITSI65188.2024.10929407
16. Zeng, J.-Y., Chang, L.-E., Cho, H.-H., Chen, C.-Y., Chao, H.-C., & Yeh, K.-H. (2022). Using Poisson distribution to enhance CNN-based NB-IoT LDoS attack detection. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)* (pp. 1–7). IEEE. https://doi.org/10.1109/DSC54232.2022.9888864
17. Hayashi, M., & Vázquez-Castro, Á. (2020). Physical layer security protocol for Poisson channels for passive man-in-the-middle attack. *IEEE Transactions on Information Forensics and Security*, *15*, 2295–2305. https://doi.org/10.1109/TIFS.2019.2963771
18. Robert, C., Carallo, G., & Casarin, R. (2021). A Bayesian generalized Poisson model for cyber risk analysis. In *Springer book chapter*. Springer. https://doi.org/10.1007/978-3-030-78965-7_19
19. Engle, R. D., Mailloux, L. O., Grimaila, M. R., Hodson, D. G., McLaughlin, C. V., & Baumgartner, G. (2019). Implementing the decoy state protocol in a practically oriented quantum key distribution system-level model. *International Journal of Telecommunication Systems*. https://doi.org/10.1177/1548512917698053
20. Goto, Y., Ng, B., Seah, W. K. G., & Takahashi, Y. (2019). Queueing analysis of software defined network with realistic OpenFlow-based switch model. *Computer Networks, 164*.
21. Zalawadia, M., Yadav, V., & Gurav, M. (2025). Comprehensive report on real-time detection of hidden communication channels in network traffic. *International Journal on Advanced Computer Engineering and Communication Technology, 14*, 26–36. https://doi.org/10.65521/ijacect.v14i2.978
22. Jayasinghe, D., Zhong, Y., & Parameswaran, S. (2025). JitFilt: Mitigate jitter-based side channel analysis attacks. In *2025 IEEE/ACM International Conference on Computer Aided Design (ICCAD)* (pp. 1–9). IEEE. https://doi.org/10.1109/ICCAD66269.2025.11241000
23. Durvaux, F., Renauld, M., Standaert, F.-X., van Oldeneel tot Oldenzeel, L., & Veyrat-Charvillon, N. (2013). Efficient removal of random delays from embedded software implementations using hidden Markov models. In S. Mangard (Ed.), *Smart card research and advanced applications: CARDIS 2012* (Lecture Notes in Computer Science, Vol. 7771). Springer. https://doi.org/10.1007/978-3-642-37288-9_9

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Harasymchuk Oleh
PhD, Associate Professor, Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-8742-8872
oleh.i.harasymchuk@lpnu.ua

MULTICRITERIA METHODOLOGY FOR SELECTING POISSON PULSE SEQUENCE GENERATORS FOR INFORMATION PROTECTION TASKS

Abstract. The paper investigates pseudo-random pulse sequence generators with a Poisson distribution law as a means of addressing specific cybersecurity and information protection tasks. A generalized structural scheme of a pseudo-random pulse sequence generator (PRPSG) and the basic classes of pseudo-random number generators used for their implementation are considered. It is substantiated that the selection of a generator cannot be based solely on the criterion of statistical compliance with the Poisson distribution, since different application scenarios impose different requirements on statistical, temporal, computational, and cryptographic characteristics. A multicriteria methodology for generator selection is proposed, taking into account statistical conformity to the Poisson process, performance, cryptographic strength, period/reproducibility, and hardware implementation feasibility. Differentiated generator requirement profiles are developed for traffic modeling, synthetic event generation, jitter generation, covert data transmission, and device authentication. A comparative analysis of MAGF, LCG, LFSR, CSPRNG, and physical sources of randomness is conducted. It is substantiated that the optimal generator class is determined by the requirements profile of a specific application scenario rather than by the existence of a universal alternative. Recommendations are formulated for selecting the appropriate generator class depending on the application scenario in information protection tasks.

Keywords: pseudo-random pulse sequence generator, Poisson process, multicriteria selection, cybersecurity, information protection, cryptographic security, statistical modeling, covert channels, device authentication.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Orúe, A. B., Hernández Encinas, L., Fernández, V., & Montoya, F. (2018). A review of cryptographically secure PRNGs in constrained devices for the IoT. In H. Pérez García, J. Alfonso-Cendón, L. Sánchez González, H. Quintián, & E. Corchado (Eds.), *International Joint Conference SOCO'17-CISIS'17-ICEUTE'17* (Advances in Intelligent Systems and Computing, Vol. 649). Springer. https://doi.org/10.1007/978-3-319-67180-2_65
2. Maksymovych, V., Shabatura, M., Harasymchuk, O., Shevchuk, R., Sawicki, P., & Zajac, T. (2022). Combined pseudo-random sequence generator for cybersecurity. *Sensors, 22*, 9700. https://doi.org/10.3390/s22249700
3. Maksymovych, V., Nyemkova, E., Justice, C., Shabatura, M., Harasymchuk, O., Lakh, Y., & Rusynko, M. (2022). Simulation of authentication in information-processing electronic devices based on Poisson pulse sequence generators. *Electronics, 11*, 2039. https://doi.org/10.3390/electronics11132039
4. Maksymovych, V., Shabatura, M., Harasymchuk, O., Karpinski, M., Jancarczyk, D., & Sawicki, P. (2022). Development of additive Fibonacci generators with improved characteristics for cybersecurity needs. *Applied Sciences, 12*, 1519. https://doi.org/10.3390/app12031519
5. Almaraz Luengo, E. (2022). A brief and understandable guide to pseudo-random number generators and specific models for security. *Statistics Surveys, 16*, 137–181.
6. Khomik, M. A., & Harasymchuk, O. I. (2024). Analysis of threats to pseudorandom number and pseudorandom sequence generators and protection measures. *Ukrainian Information Security Research Journal, 25*(4), 172–184. https://doi.org/10.18372/2410-7840.25.18222
7. Khomik, M., & Harasymchuk, O. (2023). Application of pseudorandom number and sequence generators in cybersecurity, methods of their construction and quality assessment. *Ukrainian Information Security Research Journal, 25*(3), 147–159. https://doi.org/10.18372/2410-7840.25.17940
8. Popereshniak, S. V. (2022). Methodology for statistical analysis of the randomness of sequences generated by random and pseudorandom number generators. *Telecommunication and Information Technologies, 3*(76).

9. Alani, M. M. (2010). Testing randomness in ciphertext of block-ciphers using DieHard tests. *International Journal of Computer Science and Network Security (IJCSNS), 10*(4), 53–57.
10. National Institute of Standards and Technology. (2010). *A statistical test suite for random and pseudorandom number generators for cryptographic applications* (NIST Special Publication 800-22 Rev. 1a). NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf
11. Harremoës, P. (2001). Poisson's law and information theory. In *Proceedings of the 2001 IEEE International Symposium on Information Theory* (p. 46). IEEE. https://doi.org/10.1109/ISIT.2001.935909
12. Bidiuk, P. I., Tkach, B. P., & Harrington, T. (2018). *Mathematical statistics: Textbook*. Publishing House "Personal".
13. Orúe, A. B., Montoya, F., & Hernández Encinas, L. (2010). Trifork, a new pseudorandom number generator based on lagged Fibonacci maps. *Journal of Computer Science and Engineering, 2*(2), 46–51.
14. Durga, R. S., Rashmika, C. K., Madhumitha, O. N. V., Suvetha, D. G., Tanmai, B., & Mohankumar, N. (2020). Design and synthesis of LFSR based random number generator. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 438–442). IEEE. https://doi.org/10.1109/ICSSIT48917.2020.9214240
15. Tarigan, J. T., Salim, A. C., Nababan, A. M., & Wijaya, B. (2024). Crafting the chance: Linear congruential generator in randomization system in RPGs. In *2024 International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. 270–275). IEEE. https://doi.org/10.1109/ICITSI65188.2024.10929407
16. Zeng, J.-Y., Chang, L.-E., Cho, H.-H., Chen, C.-Y., Chao, H.-C., & Yeh, K.-H. (2022). Using Poisson distribution to enhance CNN-based NB-IoT LDoS attack detection. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)* (pp. 1–7). IEEE. https://doi.org/10.1109/DSC54232.2022.9888864
17. Hayashi, M., & Vázquez-Castro, Á. (2020). Physical layer security protocol for Poisson channels for passive man-in-the-middle attack. *IEEE Transactions on Information Forensics and Security, 15*, 2295–2305. https://doi.org/10.1109/TIFS.2019.2963771
18. Robert, C., Carallo, G., & Casarin, R. (2021). A Bayesian generalized Poisson model for cyber risk analysis. In *Springer book chapter*. Springer. https://doi.org/10.1007/978-3-030-78965-7_19
19. Engle, R. D., Mailloux, L. O., Grimaila, M. R., Hodson, D. G., McLaughlin, C. V., & Baumgartner, G. (2019). Implementing the decoy state protocol in a practically oriented quantum key distribution system-level model. *International Journal of Telecommunication Systems*. https://doi.org/10.1177/1548512917698053
20. Goto, Y., Ng, B., Seah, W. K. G., & Takahashi, Y. (2019). Queueing analysis of software defined network with realistic OpenFlow-based switch model. *Computer Networks, 164*.
21. Zalawadia, M., Yadav, V., & Gurav, M. (2025). Comprehensive report on real-time detection of hidden communication channels in network traffic. *International Journal on Advanced Computer Engineering and Communication Technology, 14*, 26–36. https://doi.org/10.65521/ijacect.v14i2.978
22. Jayasinghe, D., Zhong, Y., & Parameswaran, S. (2025). JitFilt: Mitigate jitter-based side channel analysis attacks. In *2025 IEEE/ACM International Conference on Computer Aided Design (ICCAD)* (pp. 1–9). IEEE. https://doi.org/10.1109/ICCAD66269.2025.11241000
Durvaux, F., Renauld, M., Standaert, F.-X., van Oldeneel tot Oldenzeel, L., & Veyrat-Charvillon, N. (2013). Efficient removal of random delays from embedded software implementations using hidden Markov models. In S. Mangard (Ed.), *Smart card research and advanced applications: CARDIS 2012* (Lecture Notes in Computer Science, Vol. 7771). Springer. https://doi.org/10.1007/978-3-642-37288-9_9

Отримано редакцією журналу / Received: 08.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 24.09.26