

**Гарасимчук Олег Ігорович**

к.т.н., доцент кафедри захисту інформації

Національний університет "Львівська політехніка", Львів, Україна

ORCID ID: 0000-0002-8742-8872

oleh.i.harasymchuk@lpnu.ua

ЗАСТОСУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ МОДЕЛЮВАННЯ КІБЕРБЕЗПЕКОВИХ ПОДІЙ У СИСТЕМАХ ВИЯВЛЕННЯ АНОМАЛІЙ ТА ВТОРГНЕНЬ

Анотація. У роботі запропоновано підхід до формування синтетичних потоків кібербезпекових подій на основі генераторів псевдовипадкових послідовностей (ГПВП) і статистичного моделювання для задач виявлення аномалій і вторгнень у системах IDS/IPS. Розроблено математичну модель, у якій псевдовипадкова послідовність за допомогою оберненого експоненційного перетворення використовується для формування міжподійних інтервалів, а часові мітки подій отримуються їх послідовним накопиченням; кожна подія описується категорією та вектором атрибутивних характеристик. Параметри генерації визначаються режимом активності, який може бути нормальним, підвищеним або аномальним. Аномальність розглядається як багатокомпонентне відхилення, що може виявлятися у зміні інтенсивності потоку, категоріальної структури подій або статистичних характеристик їхніх параметрів. Проаналізовано межі застосовності однорідного пуассонівського наближення для моделювання складних потоків кібербезпекових подій. Розглянуто застосування моделі до трьох сценаріїв: формування навчальних і тестових наборів даних для IDS/IPS, моделювання подій для honeypot-систем і моделювання подій сканувальної активності. Сформульовано методику оцінювання статистичних властивостей і придатності сформованих потоків подій. Результати мають теоретико-методологічний характер; емпіричну перевірку моделі на реальних наборах даних визначено напрямом подальших досліджень.

Ключові слова: кібербезпека, виявлення аномалій, виявлення вторгнень, IDS/IPS, генератор псевдовипадкових послідовностей, синтетичні дані, пуассонівський процес, статистичне моделювання.

ВСТУП

Сучасні інформаційно-комунікаційні системи функціонують в умовах зростання обсягів мережевого трафіку, збільшення кількості взаємопов'язаних інформаційних ресурсів і розширення спектра кіберзагроз. Власне за таких умов забезпечення своєчасного виявлення підозрілої активності є одним із ключових завдань кібербезпеки. Системи виявлення вторгнень (Intrusion Detection Systems, IDS) [1] та системи запобігання вторгненням (Intrusion Prevention Systems, IPS) [2] широко використовуються для моніторингу подій, виявлення ознак несанкціонованої активності та реагування на потенційні інциденти. NIST розглядає мережеві, бездротові, host-based та системи аналізу мережевої поведінки як окремі класи технологій виявлення та запобігання вторгненням.

Для методів виявлення аномалій особливе значення має можливість оцінювати поведінку інформаційної системи не лише за окремими подіями, а й за часовою послідовністю їх виникнення, категоріальним складом і статистичними характеристиками. Тому під час розроблення та тестування таких методів необхідно враховувати як структуру окремої події, так і властивості потоку подій у цілому.

Особливе місце серед сучасних підходів займають методи виявлення аномалій, у яких рішення про наявність потенційної загрози приймається на основі відхилення спостережуваної поведінки від моделі нормальної активності. Дані методи дедалі частіше використовують алгоритми машинного навчання, ефективність яких значною мірою залежить від якості даних, застосованих під час розроблення, навчання та тестування. Навчальні й тестові набори мають бути репрезентативними щодо досліджуваного середовища та містити достатнє різноманіття нормальних і аномальних подій. Додатково необхідно контролювати наявність шуму, дублікатів записів і витоку інформації між навчальною та тестовою



вибірками. Тому актуальними залишаються питання якості, своєчасного оновлення та відповідності наборів даних реальному середовищу.

Незважаючи на те, що існують та широко використовуються benchmark-набори NSL-KDD [3], UNSW-NB15 [4], CICIDS2017 [5] та ToN_IoT [6], їх застосування не завжди дає змогу контролювано змінювати часову структуру подій, співвідношення класів або інтенсивність окремих типів активності, оскільки ці характеристики вже зафіксовані на етапі формування набору. Показовим є той факт, що створення таких «реальних» benchmark-наборів передбачає контрольоване формування частини трафіку: фоновий легітимний трафік CICIDS2017 спеціально генерувався на основі профілювання поведінки користувачів [5], а UNSW-NB15 поєднує реальну нормальну активність із синтетично сформованою атакувальною поведінкою, отриманою за допомогою системи IXIA PerfectStorm [4].

В якості альтернативи та доволі перспективного напрямку розв'язання проблеми доступності та контрольованості даних може бути синтетичне генерування подій кібербезпеки, які здатні відтворювати складну статистичну структуру реального трафіку. Синтетичні дані дають змогу контролювано змінювати характеристики досліджуваного середовища, регулювати співвідношення нормальних та аномальних подій, формувати рідкісні сценарії та відтворювати однакові умови експерименту. Ступінь статистичної відповідності синтетичних даних реальному трафіку залежить від використаної моделі, способу визначення її параметрів і якості вихідних даних, якщо вони застосовуються для калібрування.

Синтетичні дані, сформовані генеративними моделями, зокрема GAN, застосовуються для розширення навчальних вибірок і зменшення впливу дисбалансу класів у задачах виявлення мережових вторгнень [7]. Такі методи можуть відтворювати складні статистичні залежності реальних даних, однак якість отриманих вибірок залежить від архітектури моделі, процедури навчання, обсягу та репрезентативності вихідних даних і способу оцінювання синтетичних даних. З огляду на це для низки задач моделювання кібербезпекових подій доцільно використовувати генератори псевдовипадкових послідовностей (ГПВП) [8] у поєднанні з статистичними моделями. Застосування такого підходу дозволяє відокремити процес формування псевдовипадкових послідовностей від моделювання властивостей досліджуваного потоку подій, забезпечити високу керованість, відтворюваність і простоту інтерпретації параметрів за рахунок спрощеного відтворення складних залежностей реального трафіку. Зокрема, базову послідовність можна трансформувати в такий спосіб, щоб отримувати задані розподіли випадкових величин, а параметрами статистичної моделі визначати інтенсивність та часову структуру подій.

Для попереднього аналізу статистичних властивостей псевдовипадкових послідовностей можуть застосовуватися тести, наведені в NIST SP 800-22 Rev. 1a [9]. Водночас результати цих тестів не є доказом криптографічної стійкості генератора та не замінюють оцінювання відповідності послідовності вимогам конкретної задачі. Для застосування тестів NIST SP 800-22 до вихідних значень ГПВП необхідно попередньо сформувати відповідну бітову послідовність. Для цього можуть застосовуватися, зокрема, частотний, серійний та інші тести набору NIST SP 800-22 Rev. 1a. Результати тестування доцільно розглядати як попередню оцінку статистичних властивостей генератора, а не як підтвердження його криптографічної стійкості.

Метою даної роботи є розроблення та теоретичне обґрунтування параметризованої математичної моделі формування синтетичних потоків кібербезпекових подій на основі генераторів псевдовипадкових послідовностей і статистичного моделювання, визначення меж її застосовності та обґрунтування методики оцінювання сформованих потоків для задач виявлення аномалій і вторгнень. Особливістю запропонованого підходу є явне задання параметрів часової інтенсивності, категоріального складу та атрибутивних характеристик подій, що забезпечує контрольоване формування сценаріїв. Робота має теоретико-методологічний характер; експериментальна перевірка моделі на реальних наборах даних є напрямом подальших досліджень.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Стрімкий розвиток методів машинного та глибокого навчання для виявлення кіберзагроз зумовив підвищення вимог до обсягів, якості та репрезентативності даних, які використовуються для побудови й оцінювання систем виявлення вторгнень. На відміну від сигнатурних підходів, методи виявлення аномалій повинні формувати уявлення про нормальну поведінку інформаційної системи та виявляти відхилення від неї. Саме тому характеристики навчальної та тестової вибірок безпосередньо впливають на можливість оцінити здатність IDS виявляти раніше невідомі або недостатньо представлені типи аномальної активності. Варто зазначити, що проблеми вибору наборів даних, дисбалансу класів, застарілості окремих типів атак та відповідності набору конкретному середовищу залишаються доволі актуальними для досліджень мережевого виявлення вторгнень.



На сьогоднішній день одним з найбільш поширених підходів до дослідження систем виявлення вторгнень є використання попередньо сформованих наборів мережевих даних [10]. Їх основною перевагою є можливість відтворення експериментів на стандартизованих вибірках, порівняння різних алгоритмів та оцінювання результатів за єдиними критеріями. Серед наборів, які широко використовуються в дослідженнях IDS, можна виділити частково згадані вище:

– набір NSL-KDD [3], створений на основі вдосконалення KDD Cup 99 та тривалий час залишався одним з основних інструментів дослідження мережевого виявлення вторгнень, проте сучасні огляди відзначають його застарілість;

– набір UNSW-NB15 [4], який сформований у Cyber Range Lab Університету Нового Південного Уельсу з використанням системи IXIA PerfectStorm і засобу tcpdump та містить дев'ять категорій атак і 49 ознак мережевих потоків.

– набір CICIDS2017 [5], який вирізняється увагою до формування реалістичного фонових трафіку на основі профілів поведінки користувачів (HTTP, HTTPS, FTP, SSH, електронна пошта);

– набір CICIDS2018 [11], який містить сучасні сценарії мережевих атак і нормального трафіку, згенерованого в масштабованому середовищі, та характеризується широким набором мережевих ознак для аналізу потоків;

– набір ToN_IoT [6], який орієнтований на телеметрію IoT/IIoT-пристроїв і поєднує дані декількох рівнів мережевої інфраструктури.

Спільною ознакою згаданих наборів є те, що їх формування вже передбачає контрольоване або синтетичне відтворення частини активності, що підтверджує актуальність дослідження методів контрольованої генерації як самостійного напрямку. Для наведених наборів можна побачити важливу особливість формування даних, яка полягає в тому, що навіть у випадку подання кінцевого набору як наближеного до реального мережевого середовища, його створення часто передбачає контрольоване формування окремих компонентів трафіку. І цей факт вказує на те, що синтетичне моделювання не можна розглядати як альтернативу реальним даним у широкому сенсі, а лише як інструмент їх доповнення та контрольованого дослідження.

Порівняльний аналіз цих наборів наведено в таблиці 1.

Таблиця 1.

Порівняння наборів даних для задач виявлення мережевих атак

Набір даних	Рік	Категорії атак	Ознаки	Особливості формування
NSL-KDD	2009	4 (DoS, Probe, R2L, U2R)	41	удосконалена версія KDD Cup 99; усунено дублікати записів
UNSW-NB15	2015	9	49	сформовано з використанням IXIA PerfectStorm; поєднує реальну нормальну активність і синтетичну атакуювальну
CICIDS2017	2018	7 груп (DoS/DDoS, Brute Force, Web Attack, Infiltration, Botnet, PortScan, Heartbleed)	78 (CICFlowMeter)	фоновий легітимний трафік сформовано на основі профілів поведінки користувачів
CICIDS2018	2018	7 основних категорій	80 (CICFlowMeter)	масштабоване середовище збору даних; поєднання реалістичного фонових трафіку та різноманітних сучасних атак
ToN_IoT	2020	кілька категорій атак на IoT/IIoT	багаторівневі (мережа, host, cloud)	телеметрія IoT/IIoT-пристроїв; багаторівнева архітектура збору даних

Варто зазначити, що після 2020 року кількість доступних наборів для досліджень мережевого виявлення вторгнень суттєво зросла, проте не була усунена проблема вибору адекватного набору для конкретної задачі. Проте використання готових наборів супроводжується низкою обмежень:

– у дослідника немає можливості довільно змінювати умови їх формування після завершення збору даних;

– структура класів, співвідношення нормальної та аномальної активності, набір представлених атак і часові характеристики вже визначені авторами набору;



– набір може відображати конкретну мережеву архітектуру, набір протоколів або сценарії поведінки користувачів, а це в свою чергу обмежує перенесення отриманих результатів на інші середовища.

Також можна відзначити специфічні обмеження, помилки та проблеми з репрезентативністю окремих наборів даних.

З огляду на викладене, можна зробити висновок, що реальні та benchmark-набори залишаються необхідною основою для валідації методів IDS, але їх доцільно доповнювати контрольованими способами генерування даних. Особливо це стосується досліджень, у яких необхідно перевірити поведінку системи за умов, що відсутні або недостатньо представлені у доступних наборах.

Формування синтетичних даних може відбуватися різними способами – починаючи від простих статистичних моделей до складних генеративних нейронних мереж. Основною перевагою синтетичного підходу є можливість контролю характеристик сформованої вибірки та цілеспрямованого створення подій, які складно чи небажано отримувати шляхом реального проведення відповідних сценаріїв.

Для задач виявлення вторгнень особливо актуальною є проблема дисбалансу класів. У реальному мережевому середовищі окремі типи атак і рідкісні аномалії трапляються значно рідше за нормальну активність, через що навчальна вибірка може містити недостатню кількість прикладів окремих класів. Це значно ускладнює побудову моделей, які здатні ефективно виявляти такі події. Огляд сучасних досліджень генеративних підходів вказує на той факт, що дефіцит репрезентативних даних аномальної поведінки є однією з основних причин використання синтетичної генерації.

Іншим потужним напрямком, який викликає значний інтерес у дослідників є використання генеративних змагальних мереж та їх варіацій (Generative Adversarial Networks, GAN) [12]. У сучасних роботах GAN застосовуються для генерування синтетичних зразків атак, балансування класів, підвищення стійкості моделей та інших завдань, пов'язаних із виявленням вторгнень. Проте до основних проблем цього напрямку можна віднести нестабільність навчання, вибір гіперпараметрів, обчислювальна складність та необхідність перевірки статистичної подібності синтетичних даних до реальних. Водночас складність таких моделей не завжди є необхідною для задач, у яких досліднику потрібно не відтворити повну статистичну структуру реального трафіку, а сформувати контрольований потік подій із наперед заданими характеристиками.

Наступний напрям – це формування правдоподібного трафіку в системах кіберобману (honeypot, honeynet) [13]. Недостатня правдоподібність фонового трафіку може бути одним із чинників, що сприяють виявленню системи-пастки [14].

Четвертий напрям пов'язаний із застосуванням випадковості в задачах сканування портів і виявлення порушників. Окремим напрямом є моделювання сканувальної та іншої розвідувальної активності в задачах оцінювання IDS. Для синтетичних наборів даних такий підхід може реалізовуватися шляхом контрольованого формування подій і зміни їхньої часової та категоріальної структури.

Альтернативою генеративним нейронним мережам може бути статистичне моделювання. Його принциповою особливістю є формування даних відповідно до визначеної математичної моделі, параметри якої дослідник може змінювати. Даний підхід є надзвичайно корисним, коли потрібно дослідити вплив окремих параметрів потоку на роботу алгоритму виявлення аномалій. Вибір певної моделі залежить від характеру досліджуваної активності. Для незалежних подій, що виникають із приблизно сталою інтенсивністю, у базовій постановці може використовуватися пуассонівський процес [15]. Для потоків, що мають змінну інтенсивність, можна застосовувати неоднорідні пуассонівські процеси, а для послідовностей із вираженою залежністю між подіями необхідні вже складніші моделі.

Застосування власне статистичних моделей має суттєву перевагу з погляду відтворюваності. За фіксованого початкового стану генератора та незмінних параметрів моделі одна й та сама послідовність може бути відтворена повторно необхідну кількість разів. Це дає змогу формувати контрольовані експериментальні сценарії та окремо досліджувати вплив інтенсивності, дисперсії, часових інтервалів та інших характеристик потоку. Проте статистична модель не повинна розглядатися як точна копія реального мережевого трафіку. Реальні потоки можуть мати складну часову структуру, залежності між послідовними подіями, нерівномірність навантаження, довгі хвости розподілів та інші властивості, які не описуються простою пуассонівською моделлю. Саме тому статистичне моделювання доцільно розглядати передусім як засіб формування контрольованих сценаріїв, а не як повну заміну реальних даних.

Це розмежування можна вважати принциповим для задач виявлення аномалій. Якщо метою є дослідження реакції алгоритму на зміну інтенсивності потоку або появу статистичного сплеску, контрольована математична модель може бути достатньою. Якщо ж потрібно оцінити здатність IDS працювати в конкретній експлуатаційній мережі, синтетичні дані повинні доповнюватися реальними або високореалістичними даними.

Попри значний обсяг публікацій за кожним із зазначених напрямів, недостатньо дослідженою залишається задача побудови єдиної, явно параметризованої математичної моделі, яка поєднувала б



джерело псевдовипадковості (ГПВП), часову структуру потоку (пуассонівський процес) і категоріальну та атрибутивну структуру подій (категорія, параметри) у межах одного керованого механізму, придатного водночас для формування навчальних даних, моделювання подій для honeypot-інфраструктури та сценаріїв сканувальної активності.

Невирішеною частиною проблеми є побудова моделі, яка забезпечує незалежне параметричне керування часовою інтенсивністю потоку, категоріальним складом подій та розподілами їхніх атрибутивних характеристик. Такий поділ дає змогу формувати контрольовані сценарії відхилення від нормального режиму та окремо досліджувати реакцію алгоритмів виявлення аномалій на різні типи статистичних змін.

Наукова новизна роботи полягає в розробленні параметризованої математичної моделі формування синтетичних потоків кібербезпекових подій, у якій джерело псевдовипадкових значень, часова структура та атрибутивна структура подій представлені як окремі компоненти єдиного механізму. Запропоноване представлення дає змогу описувати аномальність як відхилення одного або кількох параметрів сценарію, не обмежуючись лише зміною інтенсивності потоку.

На відміну від підходів, що навчають генеративну модель на наявних даних, запропонована модель передбачає явне задавання параметрів сценарію. Це забезпечує керованість і відтворюваність, але саме по собі не гарантує статистичної відповідності синтетичних даних реальному трафіку. Перевірка такої відповідності має бути предметом окремого експериментального дослідження.

Генератори псевдовипадкових послідовностей у задачах кібербезпеки

Генератори псевдовипадкових послідовностей є базовим механізмом для реалізації багатьох алгоритмів статистичного моделювання. На відміну від фізичних джерел випадковості, детермінований програмний генератор за однакового початкового стану та однакових параметрів алгоритму формує ту саму послідовність вихідних значень. Ця властивість є важливою для досліджень, у яких необхідно багаторазово відтворювати однаковий сценарій або порівнювати результати різних алгоритмів на ідентичних вхідних даних.

Для задач моделювання кібербезпекових подій ГПВП може виконувати роль базового джерела псевдовипадкових значень [16]. Виконуючи подальше статистичне перетворення цих значень, можна формувати випадкові величини з необхідними розподілами. Наприклад, послідовність з рівномірним законом розподілу може використовуватися для формування експоненційно розподілених міжподійних інтервалів, які, у свою чергу, є основою для моделювання пуассонівського потоку подій.

Отже, функціонально варто розділяти два рівні моделі. На першому рівні ГПВП формує базову псевдовипадкову послідовність. На другому рівні математична модель визначає, як дана послідовність буде перетворена на конкретний потік кібербезпекових подій. Такий поділ дозволяє незалежно досліджувати якість псевдовипадкової послідовності та властивості моделі потоку.

Саме тому ми можемо розглядати ГПВП не як самостійну модель кіберзагрози, а як механізм генерації базових псевдовипадкових значень, на основі яких за допомогою статистичних перетворень формується контрольований потік кібербезпекових подій.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Математична модель формування синтетичного потоку кібербезпекових подій

Формування синтетичного потоку кібербезпекових подій виконується у три послідовні етапи:

1. Генерування базової псевдовипадкової послідовності за допомогою ГПВП;
2. Статистичне перетворення цієї послідовності у часові моменти виникнення подій;
3. Формування категоріальних та атрибутивних характеристик кожної події – її категорії та вектора атрибутивних характеристик.

На першому етапі ГПВП формує послідовність псевдовипадкових чисел $u_1, u_2, \dots$, рівномірно розподілених на інтервалі $(0; 1)$. За фіксованого початкового стану (seed) генератора та незмінних параметрів алгоритму ця послідовність детерміновано відтворюється.

Нехай U_i – псевдовипадкова величина, рівномірно розподілена на інтервалі $(0,1)$. Для формування міжподійного інтервалу використовується обернене перетворення експоненційного розподілу з параметром інтенсивності $\lambda_r > 0$:

$$X_i = -\frac{\ln U_i}{\lambda_r} \quad (1)$$

Тут X_i – інтервал часу між сусідніми подіями, а λ_r – інтенсивність потоку в режимі r . За припущення, що вихідна псевдовипадкова послідовність має властивості, близькі до незалежної



рівномірної послідовності, сформовані міжподійні інтервали моделюються як незалежні експоненційні випадкові величини з математичним сподіванням $1/\lambda_r$.

Моменти виникнення подій отримуються послідовним накопиченням інтервалів:

$$T_i = T_0 + \sum_{j=1}^i X_j \quad (2)$$

Тут T_0 – початковий момент спостереження, а T_i – час виникнення i -ї події. Такий спосіб побудови забезпечує неспадну послідовність часових міток за додатних міжподійних інтервалів.

За наведеного припущення сформовані міжподійні інтервали моделюються як незалежні експоненційні випадкові величини, тому кількість подій $N(t)$, що виникають на часовому інтервалі тривалості t , є пуассонівською випадковою величиною:

$$P(N(t) = k) = \frac{e^{-\lambda_r t} \cdot (\lambda_r t)^k}{k!}, \quad E[N(t)] = Var[N(t)] = \lambda_r t \quad (3)$$

Отже, у базовій постановці розглядається однорідний пуассонівський процес із постійною інтенсивністю λ_r . Для нього математичне сподівання та дисперсія кількості подій на інтервалі тривалості t дорівнюють $\lambda_r t$. Це припущення визначає межі застосовності моделі та не передбачає автоматичного відтворення нестационарності або залежностей між послідовними подіями.

Такий вибір є базовим припущенням моделі: він забезпечує простий та інтерпретований механізм керування інтенсивністю потоку через єдиний параметр λ_r , однак не претендує на повне відтворення складної часової структури реального трафіку.

На третьому етапі кожній події t_n додатково приписується категорія c_n , обрана відповідно до категоріального розподілу з вектором імовірностей $p = (p_1, \dots, p_k)$, $\sum p_k = 1$, та вектор параметрів $x_n = (x_n^{(1)}, \dots, x_n^{(M)})$, кожна компонента якого формується відповідно до заданого закону розподілу F_j . У базовій реалізації для кожного атрибута задається окремий маргінальний розподіл. Якщо під час генерації атрибуту формуються незалежно, це припущення має бути зафіксоване в конфігурації сценарію. Для відтворення кореляцій між характеристиками подій у подальшому можуть використовуватися спільні багатовимірні розподіли або інші моделі залежностей.

Таким чином, окрема подія набуває вигляду

$$E_i = (T_i, C_i, V_i) \quad (4)$$

а сформований потік – вигляду

$$\mathcal{E} = \{E_1, E_2, \dots, E_N\} \quad (5)$$

У цьому представленні T_i визначає час виникнення події, C_i – її категорію, а V_i – вектор атрибутивних характеристик. Сукупність n сформованих подій утворює синтетичний потік $\mathcal{E}$. Така структура відокремлює часову компоненту від категоріальної та атрибутивної, що дає змогу задавати для них окремі параметри сценарію.

Наведене розділення на три етапи є принциповим: воно дозволяє незалежно керувати джерелом псевдовипадковості, часовою інтенсивністю потоку та категоріальною й атрибутивною структурою подій, не змішуючи ці складові в одному недиференційованому механізмі генерації. Загальну схему процедури подано на рис. 1, а її покроковий запис – у вигляді алгоритму 1.

Якість псевдовипадкової послідовності та адекватність моделі подієвого потоку є різними характеристиками. Навіть якщо генератор задовольняє вибрані статистичні критерії, це не гарантує, що сформований ним потік відповідатиме властивостям реального мережевого середовища. Тому оцінювання має окремо охоплювати властивості вихідної послідовності, відповідність статистичного перетворення заданій моделі та придатність отриманих подій для конкретного сценарію дослідження.

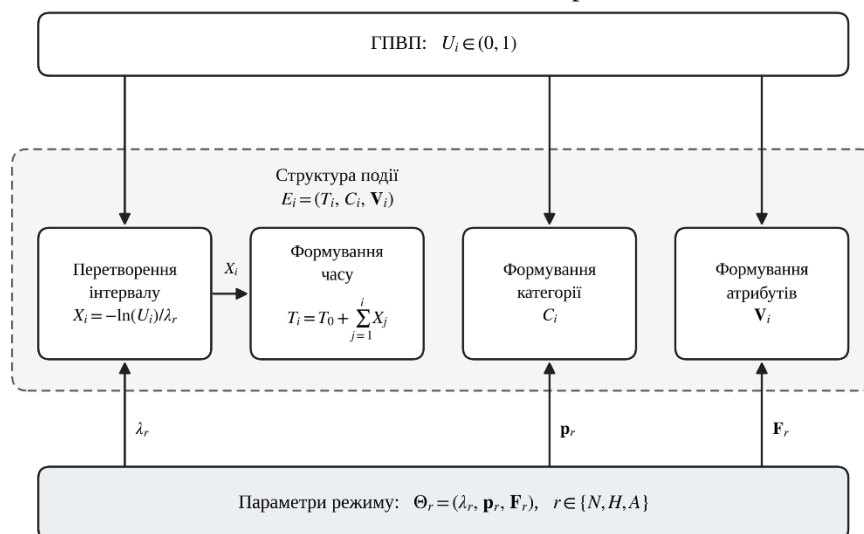


Рис. 1. Структурна схема формування синтетичного потоку кібербезпекових подій

Алгоритм 1. Формування потоку кібербезпекових подій

Вхід: початковий стан S_0 генератора; параметри режиму $\Theta_r = (\lambda_r, \mathbf{p}_r, \mathbf{F}_r)$; кількість подій n ; початковий час T_0 .

Вихід: синтетичний потік $\mathcal{E} = \{E_1, \dots, E_n\}$.

1. Ініціалізувати генератор псевдовипадкових послідовностей станом S_0 .
2. Встановити поточний час $T \leftarrow T_0$ та порожній потік $\mathcal{E}$.
3. Для $i = 1, \dots, n$ виконати:
 1. Отримати псевдовипадкове значення $U_i \in (0, 1)$.
 2. Обчислити міжподійний інтервал $X_i = -\ln(U_i) / \lambda_r$.
 3. Оновити часову мітку $T \leftarrow T + X_i$.
 4. Вибрати категорію C_i відповідно до вектора ймовірностей $\mathbf{p}_r$.
 5. Сформувати вектор атрибутів $\mathbf{V}_i$ відповідно до розподілів $\mathbf{F}_r$, використовуючи наступні значення генератора.
 6. Сформувати подію $E_i = (T, C_i, \mathbf{V}_i)$ та додати її до $\mathcal{E}$.
4. Повернути сформований потік $\mathcal{E}$.

У наведеному алгоритмі n є наперед заданою кількістю генерованих подій. Якщо моделювання має виконуватися протягом фіксованого часового інтервалу, умову завершення необхідно визначати через заданий горизонт спостереження, а не через кількість подій.

Режими активності та багатокомпонентна модель аномальності

Для моделювання різних станів досліджуваної системи введено параметричний вектор режиму

$$\theta_r = (\lambda_r, \mathbf{p}_r, \mathbf{F}_r), \quad r \in \{\text{норм}, \text{підв}, \text{аном}\}, \quad (6)$$

де λ_r – інтенсивність потоку, $\mathbf{p}_r$ – вектор ймовірностей категорій подій, $\mathbf{F}_r$ – сукупність розподілів параметрів подій у режимі r .

Принциповим результатом запропонованої моделі є те, що аномальність не зводиться лише до збільшення інтенсивності потоку. Відхилення аномального режиму від нормального доцільно розглядати як багатокомпонентну величину, що складається щонайменше з трьох окремо керованих складових:

$$K_\lambda = \frac{\lambda_A}{\lambda_N} \quad (7)$$

$$D_{TV}(\mathbf{p}_A, \mathbf{p}_N) = \frac{1}{2} \sum_{k=1}^K |p_{A,k} - p_{N,k}| \quad (8)$$

$$D_{F,j} = d(F_{A,j}, F_{N,j}). \quad (9)$$

Тут використані наступні позначення:

– λ_N, λ_A – інтенсивності нормального та аномального режимів;



- $\mathbf{p}_N, \mathbf{p}_A$ – вектори ймовірностей категорій;
- $F_{N,j}, F_{A,j}$ – розподіли j -го атрибута;
- $d(\cdot, \cdot)$ – обрана міра відстані між розподілами.

Показник K_λ характеризує відносну зміну інтенсивності потоку, D_{TV} – зміну категоріальної структури, а $D_{F,j}$ – відмінність розподілу окремого атрибута між нормальним і аномальним режимами. Значення $K_\lambda = 1$ відповідає однаковій інтенсивності двох режимів, тоді як значення, відмінне від одиниці, вказує на її зміну. Для показників D_{TV} і $D_{F,j}$ нульове значення відповідає відсутності відмінності за обраною мірою. Сукупність цих показників дає змогу формувати сценарії, у яких змінюється лише одна характеристика або декілька характеристик одночасно. Водночас ці показники описують статистичну відмінність режимів, а не безпосередньо рівень небезпечності подій.

У межах запропонованої моделі аномальність визначається як статистичне відхилення параметрів поточного режиму від базового. Тому аномальний режим не обов'язково відповідає реальній кібератаці: він може моделювати як потенційно небезпечну активність, так і легітимне, але нетипове навантаження. Віднесення конкретного сценарію до небезпечного потребує окремої предметної інтерпретації та, за можливості, перевірки на реальних даних.

Формула (7) визначає зміну інтенсивності потоку, (8) – відстань повної варіації між векторами ймовірностей категорій (зміну категоріальної структури), (9) – відмінність розподілу j -го атрибута між нормальним і аномальним режимами. Це дозволяє формувати тестові сценарії різної складності: від зміни лише одного параметра (...) до одночасної зміни всіх трьох складових, що дає змогу моделювати складніші сценарії статистичного відхилення та окремо досліджувати чутливість алгоритмів IDS до кожного типу відхилення. Якісну характеристику трьох режимів зведено в табл. 2.

Таблиця 2.

Якісна характеристика режимів активності моделі ($\theta = (\lambda_r, pr, Fr)$)

Режим	Інтенсивність	Категоріальний розподіл	Розподіли атрибутів	Призначення
Нормальний (N)	λ_N	$\mathbf{p}_N$	$\mathbf{F}_N$	Базова активність
Підвищений (H)	Може змінюватися відносно λ_N	Може залишатися близьким до $\mathbf{p}_N$	Можливі невеликі зсуви	Перевірка реакції на легітимні зміни навантаження
Аномальний (A)	λ_A	$\mathbf{p}_A$	$\mathbf{F}_A$	Контрольоване статистичне відхилення

Нормальний режим N задає базові параметри потоку. Підвищений режим H характеризується помірною зміною одного або кількох параметрів, що може відповідати легітимному сплеску активності. Аномальний режим A формується шляхом контрольованого відхилення від базового профілю. Величина відхилення не має універсального порогового значення та повинна задаватися відповідно до мети конкретного експерименту.

Можна розглянути такі сценарії застосування моделі в задачах IDS/IPS:

1. Формування навчальних і тестових наборів даних. Сформований відповідно до наведених вище потік подій E може використовуватися для побудови контрольованих навчальних і тестових наборів. Загальний набір складається з подій нормального та аномального режимів, $E = E_{\text{норм}} \cup E_{\text{аном}}$, а частка аномальних подій $a = |E_{\text{аном}}| / |E|$ є керованим параметром, що дозволяє формувати як набори з переважанням нормальної активності (типова експлуатаційна ситуація), так і збалансовані набори для методичного порівняння алгоритмів класифікації. Порівняно з інструментарієм ID2T, що ін'єктує синтетичні атаки у фоновий трафік [17], і генеративними методами подібними до SYN-GAN [7], що навчаються на реальних вибірках, запропонована модель не потребує навчальних даних для калібрування, оскільки її параметри (λ_r, pr, Fr) задаються дослідником явно. Це перевага з погляду керованості й відтворюваності, але водночас обмеження з погляду статистичної реалістичності.

2. Формування трафіку honeypot-систем. Окремим сценарієм застосування моделі є формування синтетичних подій для honeypot- та honeynet-інфраструктури. Недостатня правдоподібність фонового трафіку може бути одним із чинників, що сприяють виявленню системи-пастки. У межах цієї роботи йдеться про моделювання абстрактних подій та їхніх статистичних характеристик, а не про формування повноцінних мережевих пакетів або протокольних діалогів. Для безпосереднього використання в honeypot-інфраструктурі така модель потребуватиме інтеграції з механізмами формування трафіку та окремої перевірки правдоподібності результату. Прості реалізації такого потоку (модель з фіксованою



інтенсивністю) обчислювально дешеві, проте статистично вразливі до виявлення досвідченим зловмисником або автоматизованим детектором, що узгоджується з обмеженням, розглянутим вище.

3. *Моделювання подій сканування та іншої розвідувальної активності.* Запропонована модель також придатна для абстрактного представлення подій, характерних для сканувальної активності: аномальний сценарій у цьому разі описується не через окрему подію, а через зміну категоріальної структури потоку – збільшення частки r_k , що відповідає категорії подій розвідки (наприклад, спроб з'єднання з послідовними портами), можливо в поєднанні зі зміною інтенсивності k_k . З погляду оцінювання IDS цей сценарій дає змогу досліджувати чутливість алгоритму до зміни категоріального складу та часової інтенсивності подій. Зокрема, можна порівнювати реакцію алгоритму на зміну лише частоти подій і на зміну категоріального розподілу за незмінної загальної інтенсивності. Це дає змогу відокремити вплив різних статистичних чинників на результат виявлення.

4. *Методика оцінювання статистичних властивостей і придатності згенерованих послідовностей.* Придатність сформованого потоку подій для задач IDS/IPS доцільно перевіряти за чотирма групами критеріїв:

- статистична якість псевдовипадкової послідовності;
- відповідність часової компоненти заданій моделі;
- відповідність категоріальних та атрибутивних характеристик заданим параметрам;
- відтворюваність, керованість і прикладна придатність.

Оцінювання доцільно проводити послідовно. На першому етапі перевіряються статистичні властивості вихідної псевдовипадкової послідовності. На другому етапі оцінюється відповідність часової компоненти заданій моделі. На третьому етапі перевіряються категоріальний склад та атрибутивні характеристики сформованих подій. На четвертому етапі оцінюються відтворюваність і керованість генерації. За наявності реального набору даних додатково проводиться порівняння статистичних характеристик синтетичного та реального потоків.

Переваги, обмеження та порівняння з генеративними моделями

Порівняно з генеративними моделями штучного інтелекту [7; 12], запропонована статистична модель має інший баланс переваг і обмежень. Її основна перевага – явна керованість і інтерпретованість: кожен параметр сценарію (λ , p , F) задається дослідником безпосередньо й може змінюватися ізольовано, що забезпечує контрольований факторний аналіз чутливості IDS до окремих типів відхилень. Друга перевага – відтворюваність, що ґрунтується на фіксації початкового стану ГПВП. Генеративні моделі, навпаки, здатні відтворювати складніші багатовимірні залежності реального трафіку за умови достатнього обсягу й якості навчальних даних, однак їхні параметри визначаються в процесі навчання, а не задаються дослідником явно, що знижує інтерпретованість і потребує значних обчислювальних ресурсів.

Наведене порівняння має якісний характер і відображає концептуальні відмінності між класами підходів, а не результати експериментального тестування за єдиною кількісною методикою. Оцінки керованості, відтворюваності та обчислювальної складності залежать від конкретної реалізації, параметрів і способу використання відповідного підходу.

Таблиця 3.

Якісне порівняння запропонованої моделі з інжекцією синтетичних атак і генеративними моделями

Критерій	Запропонована статистична модель	Інжекція синтетичних атак (ID2T)	Генеративні моделі III (GAN, SYN-GAN)
Керованість параметрів	висока: явні λ , p , F	середня: параметри атаки задаються, фон визначається вхідним трафіком	низька–середня: параметри визначаються навчанням
Інтерпретованість	висока	середня	низька
Відтворюваність	висока за фіксованого початкового стану ГПВП	залежить від вхідного фонових трафіку	середня: залежить від ініціалізації та навчання
Потреба в даних	навчальні дані не потрібні	потрібен фоновий трафік	потрібна репрезентативна навчальна вибірка
Обчислювальна вартість	низька	низька–середня	можуть потребувати значних обчислювальних ресурсів під час навчання
Статистична реалістичність	обмежена	визначається реальним фоновим трафіком	потенційно висока за наявності репрезентативних даних



Основне обмеження запропонованої моделі – залежність її адекватності від обґрунтованості базових статистичних припущень, насамперед однорідності пуассонівського процесу та незалежності подій. У низці практичних задач інтенсивність потоку змінюється в часі, а поява однієї події може підвищувати ймовірність появи наступних – таку залежність однорідна пуассонівська модель принципово не відтворює. Подальший розвиток моделі може передбачати перехід до неоднорідного пуассонівського процесу з часово залежною інтенсивністю $\lambda(t)$ або до збуджених точкових процесів (Hawkes process), у яких інтенсивність залежить від попередніх подій; вибір конкретного узагальнення має визначатися характеристиками задачі, оскільки саме собою ускладнення моделі не гарантує підвищення її адекватності.

Загалом реальні дані та синтетичні дані, сформовані запропонованою моделлю, доцільно розглядати не як взаємозамінні, а як взаємодоповнювальні джерела: синтетичні потоки придатні для розширення недостатньо представлених сценаріїв, контрольованого тестування алгоритмів і дослідження їх чутливості до окремих параметрів, тоді як остаточне підтвердження практичної придатності алгоритму IDS, навченого чи протестованого на синтетичних даних, потребує перевірки на незалежних реальних або еталонних наборах.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розроблено математичну модель формування синтетичних потоків кібербезпекових подій, що поєднує генератор псевдовипадкових послідовностей як джерело базової випадковості, пуассонівський процес як механізм формування часової структури потоку та категоріальне представлення події та вектор її атрибутивних характеристик. Показано, що аномальність у межах цієї моделі доцільно розглядати як багатокомпонентне відхилення – за інтенсивністю, категоріальною структурою та статистичними характеристиками параметрів подій, – а не лише як перевищення порогового значення частоти подій.

Розглянуто три сценарії застосування моделі – формування навчальних і тестових наборів даних, моделювання подій для honeypot-систем і моделювання подій сканувальної активності – та сформульовано методику оцінювання статистичних властивостей і практичної придатності сформованих потоків подій.

Дослідження має теоретико-методологічний характер. Напрямом подальших досліджень визначено експериментальну валідацію запропонованої моделі на реальних або еталонних наборах даних, а також її розширення за рахунок неоднорідного пуассонівського процесу та збуджених точкових процесів для врахування часової нестационарності й залежності між подіями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Huynh, L., et al. (2025). Expectations versus reality: Evaluating intrusion detection systems in practice. In *2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks—Supplemental Volume (DSN-S)* (pp. 56–62). IEEE. <https://doi.org/10.1109/DSN-S65789.2025.00042>
2. Sawant, A. (2018). A comparative study of different intrusion prevention systems. In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)* (pp. 1–5). IEEE. <https://doi.org/10.1109/ICCUBEA.2018.8697500>
3. Tavallaei, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications* (pp. 1–6). IEEE. <https://doi.org/10.1109/CISDA.2009.5356528>
4. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 Military Communications and Information Systems Conference (MilCIS)* (pp. 1–6). IEEE. <https://doi.org/10.1109/MilCIS.2015.7348942>
5. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)* (pp. 108–116).
6. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access*, 8, 165130–165150. <https://doi.org/10.1109/ACCESS.2020.3022862>
7. Rahman, S., Pal, S., Mittal, S., Chawla, T., & Karmakar, C. (2024). SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security. *Internet of Things*, 26, Article 101212.
8. Хомік, М., & Гарасимчук, О. (2023). Застосування генераторів псевдовипадкових чисел та послідовностей в кібербезпеці, методи їх побудови та оцінки якості. *Захист інформації*, 25(3), 147–159. <https://doi.org/10.18372/2410-7840.25.17940>



9. 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).
10. Karatas, G., Demir, O., & Sahingoz, O. K. (2020). Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset. *IEEE Access*, 8, 32150–32162. <https://doi.org/10.1109/ACCESS.2020.2973219>
11. Ibrahimi, K., Jouhari, M., & Jakout, Z. (2024). Enhancing intrusion detection systems using machine learning classifiers on the CSE-CIC-IDS2018 dataset. In *2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM)* (pp. 1–6). IEEE. <https://doi.org/10.1109/WINCOM62286.2024.10655131>
12. Krichen, M. (2023). Generative adversarial networks. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–7). IEEE. <https://doi.org/10.1109/ICCCNT56998.2023.10306417>
13. Franco, J., Aris, A., Canberk, B., & Uluagac, A. S. (2021). A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems. *IEEE Communications Surveys & Tutorials*, 23(4), 2351–2383. <https://doi.org/10.1109/COMST.2021.3106669>
14. Morozov, D. S., Vakaliuk, T. A., Yefimenko, A. A., Nikitchuk, T. M., & Kolomiets, R. O. (2023). Honeypot and cyber deception as a tool for detecting cyber attacks on critical infrastructure. *CEUR Workshop Proceedings*, 3374, 81–96.
15. 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(13), Article 2039. <https://doi.org/10.3390/electronics11132039>
16. Maksymovych, V., Shabatura, M., Harasymchuk, O., Shevchuk, R., Sawicki, P., & Zajac, T. (2022). Combined pseudo-random sequence generator for cybersecurity. *Sensors*, 22(24), Article 9700. <https://doi.org/10.3390/s22249700>
17. Garcia Cordero, C., et al. (2019). *On generating network traffic datasets with synthetic attacks for intrusion detection (ID2T)* [Preprint]. arXiv. <https://arxiv.org/abs/1905.00304>

**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

**APPLICATION OF PSEUDORANDOM SEQUENCE GENERATORS FOR MODELING
CYBERSECURITY EVENTS IN ANOMALY DETECTION AND INTRUSION DETECTION
SYSTEMS**

Abstract. The paper proposes an approach to generating synthetic streams of cybersecurity events using pseudorandom sequence generators (PRSGs) and statistical modeling for anomaly and intrusion detection in IDS/IPS systems. A mathematical model is developed in which a pseudorandom sequence is used to generate inter-event intervals through an inverse exponential transformation, while event timestamps are obtained by cumulatively summing these intervals. Each event is characterized by a category and a vector of attributes. The generation parameters are determined by the activity regime, which may be normal, elevated, or anomalous. Anomalies are treated as multidimensional deviations that may manifest as changes in event stream intensity, the categorical structure of events, or the statistical characteristics of their parameters. The applicability limits of the homogeneous Poisson process approximation for modeling complex streams of cybersecurity events are analyzed. The proposed model is considered in three scenarios: generating training and test datasets for IDS/IPS, modeling events for honeypot systems, and simulating scanning activity events. A methodology for evaluating the statistical properties and suitability of the generated event streams is formulated. The results are theoretical and methodological in nature; empirical validation of the model using real-world datasets is identified as a direction for future research.

Keywords: cybersecurity, anomaly detection, intrusion detection, IDS/IPS, pseudorandom sequence generator, synthetic data, Poisson process, statistical modeling.

REFERENCES

1. Huynh, L., et al. (2025). Expectations versus reality: Evaluating intrusion detection systems in practice. In *2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks—Supplemental Volume (DSN-S)* (pp. 56–62). IEEE. <https://doi.org/10.1109/DSN-S65789.2025.00042>
2. Sawant, A. (2018). A comparative study of different intrusion prevention systems. In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)* (pp. 1–5). IEEE. <https://doi.org/10.1109/ICCUBEA.2018.8697500>
3. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications* (pp. 1–6). IEEE. <https://doi.org/10.1109/CISDA.2009.5356528>
4. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 Military Communications and Information Systems Conference (MilCIS)* (pp. 1–6). IEEE. <https://doi.org/10.1109/MilCIS.2015.7348942>
5. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)* (pp. 108–116).
6. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access*, 8, 165130–165150. <https://doi.org/10.1109/ACCESS.2020.3022862>
7. Rahman, S., Pal, S., Mittal, S., Chawla, T., & Karmakar, C. (2024). SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security. *Internet of Things*, 26, Article 101212.
8. Khomik, M., & Harasymchuk, O. (2023). Application of pseudorandom number and sequence generators in cybersecurity: Methods of their construction and quality assessment. *Information Security*, 25(3), 147–159. <https://doi.org/10.18372/2410-7840.25.17940>
9. 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).



10. Karatas, G., Demir, O., & Sahingoz, O. K. (2020). Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset. *IEEE Access*, 8, 32150–32162. <https://doi.org/10.1109/ACCESS.2020.2973219>
11. Ibrahimi, K., Jouhari, M., & Jakout, Z. (2024). Enhancing intrusion detection systems using machine learning classifiers on the CSE-CIC-IDS2018 dataset. In *2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM)* (pp. 1–6). IEEE. <https://doi.org/10.1109/WINCOM62286.2024.10655131>
12. Krichen, M. (2023). Generative adversarial networks. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–7). IEEE. <https://doi.org/10.1109/ICCCNT56998.2023.10306417>
13. Franco, J., Aris, A., Canberk, B., & Uluagac, A. S. (2021). A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems. *IEEE Communications Surveys & Tutorials*, 23(4), 2351–2383. <https://doi.org/10.1109/COMST.2021.3106669>
14. Morozov, D. S., Vakaliuk, T. A., Yefimenko, A. A., Nikitchuk, T. M., & Kolomiiets, R. O. (2023). Honeypot and cyber deception as a tool for detecting cyber attacks on critical infrastructure. *CEUR Workshop Proceedings*, 3374, 81–96.
15. 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(13), Article 2039. <https://doi.org/10.3390/electronics11132039>
16. Maksymovych, V., Shabatura, M., Harasymchuk, O., Shevchuk, R., Sawicki, P., & Zajac, T. (2022). Combined pseudo-random sequence generator for cybersecurity. *Sensors*, 22(24), Article 9700. <https://doi.org/10.3390/s22249700>
17. Garcia Cordero, C., et al. (2019). *On generating network traffic datasets with synthetic attacks for intrusion detection (ID2T)* [Preprint]. arXiv. <https://arxiv.org/abs/1905.00304>

Отримано редакцією журналу / Received: 08.09.26

Прорецензовано / Revised: 20.09.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.