Войтко Тетяна Миколаївна, науковий співробітник науково-дослідного відділу Інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України.

Tetiana Voitko, Researcher of the Research Department, Institute of Information and Communication Technologies and Cyber Defense, National Defence University.
E-mail: t.voytko@ukr.net.
Orcid ID: 0000-0002-4326-0633.

Оленюк Дмитро Олександрович, аспірант, асистент кафедри комп'ютерних технологій і моделювання систем Поліського національного університету.

Dmytro Oleniuk, Postgraduate student, Assistant of Computer Technology and Systems Modeling Department, Polissia National University.
E-mail: omuzif@gmail.com.
Orcid ID: 0000-0002-9641-3795.

DOI: 10.18372/2410-7840.25.17940
УДК 004.056.5

ЗАСТОСУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ТА ПОСЛІДОВНОСТЕЙ В КІБЕРБЕЗПЕЦІ, МЕТОДИ ЇХ ПОБУДОВИ ТА ОЦІНКИ ЯКОСТІ

Марія Хомік, Олег Гарасимчук

У зв'язку з бурхливим розвитком обчислювальної і вимірювальної техніки, а також із впровадженням новітніх технологій значно розширилась сфера застосування генераторів псевдовипадкових чисел та псевдовипадкових послідовностей, що ставить нові вимоги до їх проектування та методів оцінки якості. Якісні псевдовипадкові послідовності, хоча і є за своєю суттю детермінованими, володіють проте практично всіма властивостями реалізацій істинно випадкових процесів і успішно їх замінюють, оскільки формування випадкових послідовностей надзвичайно складне. У зв'язку з різноманітністю і широким спектром завдань, які потребують використання псевдовипадкових числових послідовностей, постійно розробляються і вдосконалюються нові алгоритми, методи і засоби для отримання таких послідовностей. За допомогою генераторів псевдовипадкових послідовностей можна отримувати послідовності чисел, де кожен елемент практично незалежний від інших і відповідає певному заданому закону розподілу, найбільш поширеним з яких є рівномірний закон розподілу. Завдяки своїм статистичним властивостям та швидкості генерації генератори псевдовипадкових чисел та послідовностей є важливим інструментом для багатьох сфер діяльності: імітаційного моделювання (економічні, математичні, фізичні, медичні дослідження, військова справа), розробок комп'ютерних ігор (генерація 3D-моделей, текстур та світів, а також створення різноманітності та випадковості у поведінці персонажів та подій), вимірювальної техніки. Загалом важливо відзначити, що розробники генераторів псевдовипадкових послідовностей стикаються з низкою жорстких вимог, щодо певних характеристик результатів, які вони створюють за допомогою цих генераторів. Ці вимоги можуть варіюватися залежно від конкретного призначення генератора, і в разі використання псевдовипадкових послідовностей у сферах кібербезпеки та захисту інформації, вони можуть бути особливо високими і вимогливими. Наприклад, для криптографічних застосувань вимоги є надзвичайно суворими і часом навіть протирічать одна одній. Для перевірки відповідності згенерованої послідовності заданим критеріям та вимогам необхідно провести оцінювання її якості, під час якого проводиться оцінювання за різними ознаками та параметрами. Оскільки при розробці генераторів псевдовипадкових послідовностей прагнуть досягти того, щоб вони були схожі на послідовності чисел, що розподіляються дійсно випадково, то в основі будь-якого оцінювання генераторів лежить порівняння статистичних характеристик згенерованої послідовності з характеристиками істинно випадкових послідовностей. З цією метою використовуються різноманітні тести, які дозволяють виявляти наявні статистичні закономірності і, таким чином, виявляти низьку якість згенерованих псевдовипадкових послідовностей.

***Ключові слова**: генератори псевдовипадкових чисел, генератори псевдовипадкових послідовностей, кібербезпека, генерування, тестування, оцінювання якості.*

ВСТУП

Швидкий розвиток інформаційних технологій та засобів обчислювальної техніки значно розширив сферу застосування випадкових чисел та послідовностей та підвищив вимоги, які висуваються до пристроїв їх генерування.

На сьогоднішній день генератори псевдовипадкових чисел (ГПВЧ) та псевдовипадкових послідовностей (ГПВП) є надзвичайно поширені та використовуються в багатьох галузях науки та технологій. Вони відіграють важливу роль в обчислювальній та вимірювальній техніці, при моделюванні різноманітних процесів, при вирішенні промислових задач та для задач кібербезпеки, актуальність яких зростає із кожним роком.

Серед таких задач можна виділити: задачі шифрування інформації, генерування секретних ключів, аутентифікації, конфіденційності та забезпечення цілісності інформації, в різних методах зашумлення та захисту для забезпечення безпеки, конфіденційності та надійності інформації. Усі ці перелічені завдання неможливо вирішити без застосування ГПВЧ та ГПВП.

В першу чергу таке широке застосування можна пояснити тим, що більшість з них відповідають наступним критеріям: випадковість, що передбачає проходження усіх статистичних тестів на випадковість; керованість, що полягає у можливості відтворення випадкового потоку виведення, за бажанням; портативність, коли існує можливість створювати однакові результати на різноманітних комп'ютерних системах; ефективність – велика швидкодія, мінімальні вимоги до комп'ютерних ресурсів та документація, коли такі генератори теоретично проаналізовані та ретельно досліджені.

Основне призначення таких генераторів полягає у створенні послідовностей чисел, які здаються випадковими, проте зберігають детермінований характер.

Загалом, генератори псевдовипадкових послідовностей відіграють критичну роль у різних аспектах захисту та безпеки інформації, забезпечуючи випадковість та надійність в криптографічних та інших застосуваннях. Якісні псевдовипадкові послідовності, будучи за своєю суттю детермінованими, володіють проте практично всіма властивостями реалізацій істинно випадкових процесів і успішно їх замінюють, оскільки випадкові послідовності надзвичайно складно формувати. Постановка завдання полягає в аналізі сучасних методів та способів побудови генераторів псевдовипадкових чисел та послідовностей, сфер застосування у кібербезпеці та методів оцінки їх якості. Основною метою є структурування методів застосування таких генераторів для вирішення задач кібербезпеки. Для досягнення даної мети необхідно проаналізувати можливі способи та форми використання таких генераторів в конкретних завданнях, основні методи їх побудови та оцінки шляхом аналізу останніх досліджень і публікацій в даній тематиці та розробити узагальнюючу класифікацію на основі такого аналізу. Отримані результати можуть бути використані фахівцями з кібербезпеки, сфери діяльності яких потребують псевдовипадкових чисел та генераторів, що їх продукують.

Дослідженням методів побудови ГПВЧ та ГПВП, сферам їх використання та оцінки якості присвячена велика кількість праць як українських так і закордонних науковців та дослідників, зокрема [1-8]. Аналізуючи ці праці можна побачити, який широкий спектр застосування даних генераторів.

Якщо мова йде про використання в задачах захисту інформації, то особливо варто виділити, той факт, що для сучасних програм шифрування та безпеки генератори випадкових чисел та бітових послідовностей, та самі підходи до їх побудови, мають вирішальне значення та носять критичний характер [9]. Генерування випадкових послідовностей із заданим ймовірнісним законом та перевірка їх адекватності – одні з найважливіших проблем сучасної криптології. Наукова і практична значимість цієї проблеми настільки велика, що їй присвячені окремі монографії в області криптології, організовуються розділи в наукових журналах.

ГПВЧ та ГПВП використовуються як складові блоки, а також окремо для вирішення широкого спектру завдань захисту інформації [10-14].

Випадкові числа є важливим вхідним матеріалом для багатьох функцій Інтернету речей (IoT) [15-18].

В роботі [19] запропоновано текстовий алгоритм водяних знаків на основі генератора псевдовипадкових чисел (PRNG) для застосування в криптографії. який має хорошу невидимість і надійність, щоб протистояти видаленню, атаці модифікації тощо, а також його можна застосувати в області приховування інформації за допомогою хмарних обчислень.

У [20] автори зосереджуються на ризиках для безпеки та конфіденційності в хмарних базах даних і пропонують рішення для клієнтів, які хочуть спільно генерувати псевдовипадкові числа розподіленим способом, який може бути достатньо безпечним, швидким та малозатратним для задоволення вимог хмарної бази даних. У [21] автори представляють новий підхід до впровадження генераторів псевдовипадкових чисел, пропонуючи використовувати генеративні змагальні мережі (GAN) для навчання нейронної мережі з метою досягнути, щоб її поведінка нагадувала ГПВЧ.

ОСНОВНА ЧАСТИНА

Основні вимоги до ГПВЧ та ГПВП та методи їх побудови

Загальними вимогами до характеристик ГПВЧ та ГПВП, під час їх проектування та побудови, є наступні:

– максимальний період повторення, якщо йде мова про псевдовипадкові рівномірно розподілені числа;

– максимальна простота реалізації;

– висока швидкодія;

– задовільні статистичні властивості.

Якщо мова йде про використання ГПВЧ чи ГПВП в задачах захисту інформації, то до нього висуваються додаткові вимоги, які є фундаментом, що забезпечує їхню ефективність, надійність та стійкість до атак, зокрема:

– непередбачуваність (фактично криптографічний стійкість);

– задовільні статистичні властивості – значення, які формуються на виході ідеального ГПВП повинні мати рівномірний закон розподілу, та не повинно бути кореляції. Тобто згенерована псевдовипадкова послідовність за своїми статистичними характеристиками не повинна відрізнятись від істинно випадкової послідовності;

– великий період повторення згенерованої послідовності, що гарантує відсутність зациклювання послідовності в межах розв'язуваної задачі;

– генератор псевдовипадкових чисел має створювати послідовність, яка не містить прихованих періодичних закономірностей та характеризується рівномірним спектром;

– можливість ефективної реалізації в програмному та апаратному виконанні.

– висока швидкодія – завжди повинна бути ефективна реалізація ГПВП з точки зору швидкості обчислення та використання оперативної пам'яті;

– відтворюваність – інколи необхідно мати можливість згенерувати одну і ту ж послідовність багаторазово;

– переносимість – це можливість формувати одну і ту ж ПВП на різних програмно-апаратних платформах;

– портативність, тобто такі генератори повинні працювати однаково на різному устаткуванні та операційних системах.

Обов'язковим вважається виконання ряду наступних вимог: криптографічна стійкість, хороші статистичні властивості, швидкість отримання наступного елемента при відомому попередньому (для поділу послідовності на кілька потоків). Реалізація даного генератора має бути ефективною й стосовно апаратних ресурсів, адже існує необхідність його використовування на таких пристроях як: електронний ключ, смарт-карта тощо.

З огляду на кількість вимог, можна стверджувати, що розробити по-справжньому якісний генератор псевдовипадкових чисел дуже важко.

Постійне зростання вимог до апаратних та програмних засобів, в структурі яких є ГПВЧ чи ГПВП, спонукає дослідників до пошуку нових підходів по їх проектуванню, оптимізації структур існуючих генераторів та покращення їх характеристик. Тому в даному напрямку науковцями проводиться активна робота, яка охоплює різні можливі аспекти.

Покращити характеристики ГПВЧ та ГПВП можна шляхом:

– оптимізації параметрів ГПВЧ та ГПВП з метою покращення їх характеристик і усунення надлишковості;

– розроблення нових структур і алгоритмів роботи ГПВЧ та ГПВП, які б дозволяли їх апаратну реалізацію з підвищеною швидкодією, збільшеним періодом повторення (для ГПВП), задовільними статистичними характеристиками, підвищеною криптостійкістю;

– розробка структур ГПВЧ та ГПВП подвійного використання, зокрема, генераторів, які можна було б ефективно застосовувати як для вирі-

шення завдань кібербезпеки так і, наприклад, для формування імпульсних потоків із законом розподілу, що відрізняється від рівномірного з метою застосування в інших областях науки та техніки.

В основі роботи ГПВЧ та ГПВП лежить процес генерації, який вимагає вхідних параметрів, відомих як "насіння". Якість і точність генерованої послідовності визначається саме цим насінням. У контекстах, де непередбачуваність критична, важливо, щоб воно було по-справжньому випадковим та непередбачуваним.

За допомогою складних математичних та логічних трансформацій ГПВЧ намагаються максимально наблизити свої випадкові послідовності до справжнього випадкового вигляду. Ці перетворення забезпечують покращення статистичних характеристик послідовностей та інколи роблять їх вигляд більш випадковими, ніж навіть числа, отримані з фізичних джерел.

Однак, необхідно пам'ятати, що усі послідовності, створені ГПВЧ, все ж є детермінованими. Це означає, що весь випадковий характер обмежений самим процесом генерації насіння. Якщо воно відоме, ми зможемо точно відтворити всю послідовність [22].

Сьогодні існує багато методів побудови ГПВЧ. Найбільш поширеними є наступні методи: лінійний конгруентний метод, інверсний конгруентний, метод серединних квадратів, LFSR-генератори, вихор Мерсена, адитивний генератор, рандомізація перемішуванням, метод генерування на основі скінченних полів та ряд інших [4-5].

Лінійний конгруентний метод – це один з найпростіших і найбільш відомих методів генерації псевдовипадкових чисел. Основна ідея методу полягає у тому, щоб генерувати послідовність чисел за допомогою рекурсивної формули, де кожен наступний член послідовності обчислюється на основі попереднього члена.

Основні параметри лінійного конгруентного методу включають:

– Початкове значення (seed): початковий елемент, від якого розпочинається генерація послідовності.

– Коефіцієнти a, c і m: ці параметри визначають рекурсивну формулу для генерації нових чисел. Коефіцієнт "a" називається множником, "c" – приростом, а "m" - модулем. Формула виглядає наступним чином:

$$X_{i+1} = (a * X_i + c) \bmod m. \quad (1)$$

Діапазон генерованих значень визначає, які значення будуть міститися в послідовності. Зазвичай це числа від 0 до (m - 1).

Для успішної роботи лінійного конгруентного методу важливо вдало обирати відповідні значення для параметрів "a", "c" і "m". Погано підібрані параметри можуть призводити до послідовностей, які мають недостатню випадковість або виводяться в цикли. Крім того, генеровані числа можуть мати обмежену довжину періоду, після якого послідовність починає повторюватися.

Застосування лінійного конгруентного методу в криптографічних задачах може бути обмеженим через вразливості до криптоаналізу. Оскільки генератори цього типу мають деяку детермінованість, вони можуть бути піддані атакам, які використовують статистичний аналіз або інші методи для визначення параметрів генератора.

Взагалі, лінійний конгруентний метод може бути корисним у випадках, де важливо швидко генерувати псевдовипадкові числа для необхідних обчислень, але варто ретельно підходити до вибору параметрів та враховувати його обмежену криптографічну стійкість.

Інверсний конгруентний метод є одним із підходів до генерації псевдовипадкових чисел, який базується на оберненому використанні конгруентної функції для створення послідовності чисел з бажаними властивостями. Він заснований на ідейній протилежності до стандартного лінійного конгруентного методу, де замість генерації наступного числа з поточного за допомогою конгруентної формули використовується обернена операція.

Основний недолік інверсних генераторів полягає в їхній трудоємності, особливо в операції обернення елемента в кінцевому полі.

Обернення елемента вимагає значних обчислювальних ресурсів та часу, що може вплинути на швидкодію генератора. Також у деяких випадках, операція обернення може бути навіть неможливою або дуже обтяжливою, зокрема при великих модулях.

Незважаючи на цей недолік, інверсний конгруентний метод має певні переваги. Він дозволяє забезпечити високий ступінь статистичної незалежності та криптографічної стійкості генерованих чисел. Деколи операція обернення не є критичною для швидкодії програми, тоді інверсний конгруентний метод може бути застосований для отримання випадкових чисел з властивостями, які важко досяжні іншими методами.

Метод серединних квадратів є одним зі старіших та простих методів генерації псевдовипадкових чисел. Він був запропонований Френсісом Голтоном у 1889 році і є однією з перших спроб генерувати псевдовипадкові числа за допомогою обчислювальних машин. Принцип методу полягає у послідовному піднятті числа до квадрату, а потім взятті центральних цифр з отриманого квадрату як наступного числа у послідовності. Основна ідея використання центральних цифр полягає в тому, що якщо початкове число недостатньо випадкове, то результат піднесення його до квадрату буде містити більше випадковості.

Хоча метод серединних квадратів простий у реалізації, він має деякі серйозні недоліки:

– Залежно від початкового числа, можуть виникати циклічні послідовності, коли генератор повторює певний цикл чисел.

– Якщо початкове число має низьку ентропію або нерівномірний розподіл цифр, це може призвести до низької якості згенерованих чисел.

– Використання лише центральних цифр може призводити до зменшення властивостей випадковості у великих послідовностях.

Ще один алгоритм генерації псевдовипадкових чисел – вихор Мерсена. Він володіє великою довжиною періоду, високою якістю генерованих чисел та хорошою швидкодією, що робить його одним із найпопулярніших генераторів у багатьох програмних застосунках. Основна ідея методу вихора Мерсена полягає в використанні рекурсивної лінійної рекурентної послідовності над скінченним полем з простим модулем, яка згодом модифікується та перемішується, щоб забезпечити високу якість генерованих чисел.

Адитивні генератори Фібоначчі дуже ефективні, оскільки їх результатом є випадкові слова, а не випадкові біти. Самі по собі вони не являються криптографічно стійкими, але їх можна використовувати в якості складових блоків для безпечних генераторів.

Щодо рандомізації перемішуванням, то це важливий клас методів, заснованих на комбінуванні генераторів випадкових чисел. Однак методи перемішування мають серйозний недолік - вони змінюють порядок слідування чисел, але не самі числа.

Одним з найпростіших методів отримання псевдовипадкових рівномірно розподілених чисел є генерування за допомогою генераторів М-послідовностей. Такі генератори ще називають генераторами псевдовипадкових чисел на лінійних послідовнісних машинах (ЛПМ), або генераторами на основі регістрів зсуву з лінійними зворотними зв'язками – LFSR (Linear Feedback Shift Register). Питаннями побудови таких генераторів вчені займаються давно і цьому напрямку, на даний час, присвячено ряд праць [23-25].

Вище перелічені методи генерації псевдовипадкових чисел є серед найпоширеніших, проте варто відзначити, що це лише частина розмаїття наявних методів. Загалом, існує безліч інших різних підходів, які можна узагальнити у два основних класи: криптостійкі та некриптостійкі [4].

Криптостійкі методи призначені для застосування в криптографічних задачах, де важливість високої випадковості та непередбачуваності є визначальною. Вони можуть бути побудовані на основі поточних шифрів (генератори SEAL, RC4, RC5, RC6, Grain, Yamb, Phelix та інші), блокових шифрів (Гост 28147-89, AES, ANSI X9.17, DES), односторонніх функцій (генератори BBS, RSA, Dual_EC_DRBG, GPSSD).

Некриптостійкі методи, натомість, можуть використовуватися в менш вимогливих сценаріях, де важливість статистичних властивостей та високої продуктивності переважає над вимогами криптографічної стійкості. Такі методи можуть бути побудовані на основі елементарних рекурентів (лінійний, поліноміальний конгруентні генератори,

мультиплікативний генератор Фібоначчі із запізненням тощо) та на основі операцій в кінцевих полях (генератор Галуа, генератор Де Брейна, генератор Фібоначчі, адитивний генератор, генератор Голмана, стискаючий генератор тощо).

Кожен з цих класів має свої особливості та застосування, і вибір найбільш придатного методу залежить від конкретних вимог та використання.

Використання ГПВЧ та ГПТВ в задачах кібербезпеки

У сфері кібербезпеки ГПВЧ є критичними інструментами, які забезпечують захист та конфіденційність у різних аспектах інформаційної безпеки. Нижче відображено запропоновану нами структуру, яка показує основні сфери застосування таких генераторів в кібербезпеці (рис. 1).

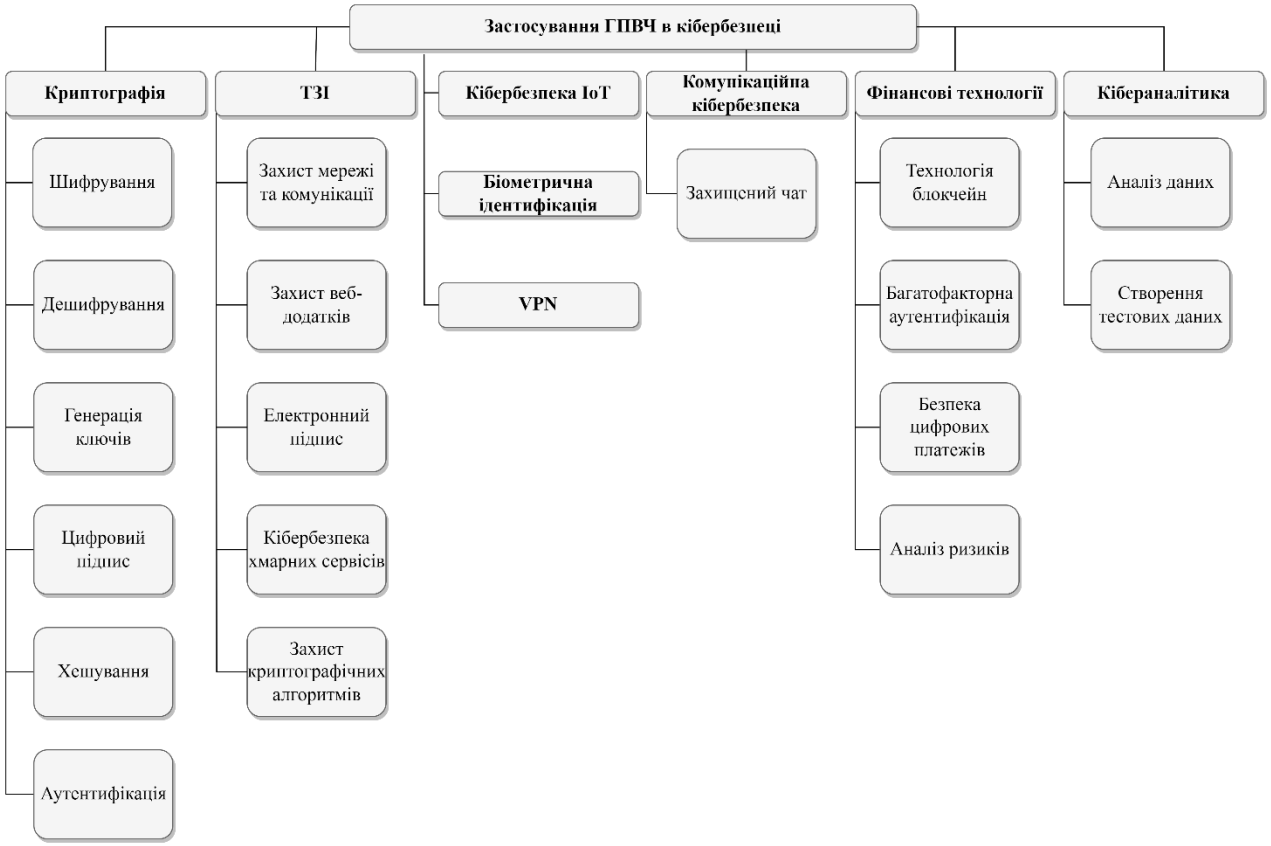

Рис. 1. Застосування ГПВЧ та ГПВП в кібербезпеці

Дана структура показує, що генератори псевдовипадкових чисел є невід'ємною частиною кібербезпеки у криптографії [1,3,19,26]. Вони допомагають створювати стійкі криптографічні протоколи та забезпечують конфіденційність, цілісність та автентичність даних. ГПВЧ використовуються для генерації випадкових ключів, ініціалізаційних векторів та інших параметрів, необхідних для шифрування, дешифрування даних, цифрових підписів, аутентифікації. Вони також використовуються в хешуванні для створення солі (salt) – додаткових випадкових даних, які додаються до вхідного повідомлення перед хешуванням. Сіль допомагає забезпечити унікальність хешів для однакових повідомлень і ускладнює злам хеш-функції методами, такими як: атака перебором або атака зі словником. Криптографічні хеш-функції використовуються в багатьох кібербезпечних сценаріях, таких як: збереження паролів, цифровий підпис, перевірка цілісності даних тощо.

ГПВЧ є важливою складовою ТЗІ (технічного захисту інформації) [26], тому існує безліч прикладів застосування у цій галузі. Дані генератори є необхідні для безпеки мережі та комунікації. Вони використовуються для захисту веб-додатків, які потребують випадкових токенів та ідентифікаторів

для зниження ризиків їх зламу, забезпечення безпеки сесій, запобігання атак перебору паролів.

ГПВЧ забезпечують випадкові числа для створення електронних підписів. У хмарних сервісах довірливість генератора псевдовипадкових чисел відіграє критичну роль у захищеності даних та ідентифікації користувачів.

Такий генератор використовується і для створення випадкових даних, що тестують та перевіряють ефективність криптографічних алгоритмів. Це допомагає перевірити той факт, що алгоритми захисту даних є дійсно стійкими.

Генератори псевдовипадкових чисел присутні у розумних пристроях та Інтернеті речей [16-18, 27]. IoT привносить мережевий інтелект у фізичні речі навколо нас, тому особливо гостро постає питання безпеки. Не менш важливим є захист приватного життя і персональних даних, доступ до яких зловмисники можуть отримати через злам систем промислово побутової автоматизації, моніторингу, безпеки і контролю доступу (технології smart home), wearable-електроніки (фітнес-трекерів, розумних годинників, окулярів), домашньої електроніки тощо. IoT-пристрої можуть бути не лише об'єктом атаки, але і суб'єктом, наприклад, IoT-ботнети використовуються зловмисниками для організації DDoS-атак, поширення вірусів тощо. Щоб захистити рішення IoT, потрібно забезпечити захист пристроїв, їх підключення до хмари, конфіденційність даних в хмарі під час передачі, обробки і зберігання, а також стійкість до віртуальних і фізичних атак. В Інтернеті захист даних від несанкціонованого доступу і збереження інформації своїх основних властивостей (конфіденційність, автентичність та цілісність) реалізується криптографічними методами шифрування та хешування. Разом з тим для вироблення ключів та векторів ініціалізації використовуються генератори випадкових та псевдовипадкових чисел.

ГПВЧ та ГПВП знайшли широке застосування в біометрії [28], особливо при використанні різних біометричних ознак. Наразі існує більше десятка різних біометричних методів, таких як: відбитки пальців, райдужна оболонка ока та інші, і для них використовуються різні типи сканерів з різними принципами роботи. ГПВЧ та ГПВП можуть бути використані для створення унікальних ключів або шаблонів, які організовують безпеку та конфіденційність біометричних даних під час їх передачі, обробки та зберігання.

Вибір і застосування надійних та криптографічно стійких ГПВЧ та ГПВП є важливим завданням для компаній, що розробляють VPN-рішення. Ненадійні генератори псевдовипадкових чисел можуть підірвати всю безпеку системи і спричинити потенційні ризики для користувачів. В [29] проаналізовано ситуацію, що трапилась у грудні 2015 року. Компанія Juniper Networks оголосила про численні вразливості безпеки, що стосувалися операційної системи ScreenOS, використовуваної у їхніх маршрутизаторах NetScreen VPN. Однією з цих уразливостей стала можливість пасивного дешифрування VPN, яка була включена через зміну точки еліптичної кривої, що використовується генератором псевдовипадкових чисел Dual EC. Ця вразливість в генераторі псевдовипадкових чисел Dual EC дозволяла атакуючим здійснювати пасивне дешифрування трафіку, що протирічило основним цілям безпеки VPN. Цей випадок став прикладом того, наскільки ГПВЧ і їхня безпека є важливими для VPN.

Генератори псевдовипадкових чисел відіграють важливу роль в комунікаційній кібербезпеці. Прикладом їх застосування є захищений чат [30], який гарантує безпечну комунікацію між користувачами. Через подібні чати можна надсилати файли, картинки, посилання та відео, здійснювати аудіо та відео дзвінки. Повідомлення шифруються і не зберігаються на серверах, а кожна розмова користувачів є тимчасовою, і сенс автоматично видаляється після завершення. Такі відомі месенджери як Telegram та Viber мають подібний функціонал, але в нього обмежені можливості і доступний він лише на смартфонах. Захищеність забезпечують не тільки шифрування повідомлень, а й генерація унікального ключа сесії. Ключ втрачає актуальність в момент завершення сеансу чата. Генерація здійснюється генератором псевдовипадкових чисел, якому задано зерно та достатня ентропія, що забезпечують криптографічну стійкість та продуктивність.

Забезпечення безпеки та захисту даних у різних аспектах фінансових технологій також пов'язане з ГПВЧ. Такі генератори потрібні в першу

чергу для технології блокчейн [31], адже вона є однією з ключових компонентів фінансових технологій. Блокчейн – це розподілена, децентралізована база даних, що забезпечує надійне зберігання і передачу інформації між користувачами без посередництва центральної влади. Ця технологія заснована на криптографічних принципах та використовує групу записів, відомих як блоки, які поєднуються в послідовний ланцюжок. Кожен блок містить дані та унікальний ідентифікатор (хеш) попереднього блока, що робить ланцюжок невідредагованим і безпечним. Технологія блокчейн забезпечує безпеку, відкритість та недоступність до втручання. Оскільки дані розподілені між багатьма учасниками мережі, зміни в блоках мають бути погоджені більшістю мережі, що ускладнює можливість фальсифікації даних. Таким чином, блокчейн може слугувати базою даних для реєстрації транзакцій, активів або будь-яких даних, які потребують високого рівня безпеки та перевірки. Генератори псевдовипадкових чисел є важливими в технології блокчейн. Оскільки блокчейн базується на криптографічних принципах, відповідність важливих криптографічних протоколів залежить від якості випадкових чисел. Крім того ГПВЧ також використовуються у фінансових технологіях для цифрових підписів, багатофакторної аутентифікації, безпеки цифрових платежів, аналізу ризиків тощо.

Генератори псевдовипадкових чисел застосовуються в кібераналітиці для різних завдань та аспектів обробки і аналізу даних з метою виявлення кіберзагроз та покращення кібербезпеки. Вони допомагають при створенні тестових даних та подій, які забезпечують непередбачуваність, різноманітність та випадковість в аналітичних даних, що покращує точність та ефективність методів кібераналітики.

Методи оцінки якості ГПВЧ та ГПВП

Оскільки існує велика кількість ГПВП, то доцільно проводити дослідження щодо їх якості, а також – з метою виявлення найкращих варіантів їх побудови для практичної реалізації чи конкретного застосування.

Щоб оцінити згенеровану псевдовипадкову послідовність або виявити, який метод генерування криптостійкий, а який ні, проводиться тестування та оцінювання якості вихідних послідовностей. Це дозволяє виявити можливі недоліки та вразливості у їх роботі, такі як: циклічність, слабкі статистичні властивості або недостатню криптографічну стійкість. Тестування особливо важливо для криптографічних систем, адже недоліки в генерації випадкових чисел можуть використовуватися атакуючими для порушення безпеки. Оцінювання якості також допомагає визначити, наскільки добре відповідає генератор та послідовність на його виході потребам конкретного застосування, допомагаючи розробникам вибрати найбільш ефективний метод.

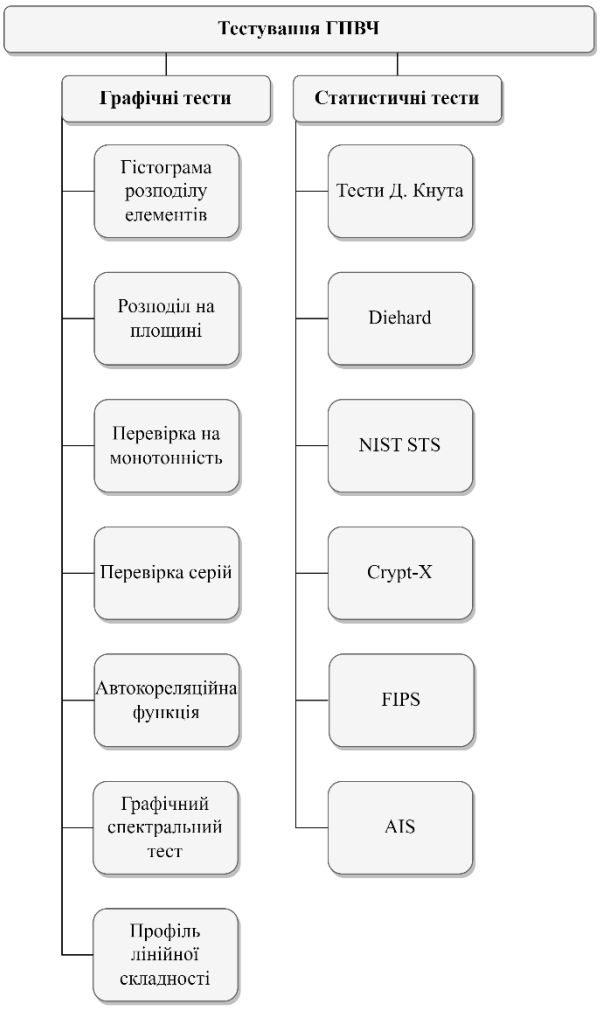

Рис. 2. Методи тестування ГПВЧ та ГПВП

Тестування генераторів псевдовипадкових чисел включає наступні види тестів: емпіричні, теоретичні, прикладні [5, 15, 22, 32-40].

У першому випадку машини оперують групами чисел у послідовності та оцінюють їх якість за допомогою визначених статистичних критеріїв. Ці тести ґрунтуються на практичних даних та допомагають з'ясувати, наскільки випадкові числа генеруються алгоритмом.

Теоретичні тести схожі на емпіричні тести, але оцінка якості ГПВЧ базується на абстрактних статистичних властивостях. Вони використовують математичні моделі для визначення очікуваних властивостей генератора.

Прикладні тести перевіряють придатність алгоритму для конкретних прикладних програм. Вони базуються на відомих аналітичних результатах, що можуть бути вираховані для визначених ситуацій.

Загалом можна виділити графічні та статистичні методи (рис. 2), які використовуються для оцінки якості ГПВЧ та ГПВП [5].

Графічні методи є ефективним способом візуалізації характеристик послідовностей. Вони включають в себе гістограми розподілу елементів, розподіли на площині, перевірку на монотонність, перевірку серій, автокореляційну функцію, графічний спектральний тест, профіль лінійної складності:

– гістограма дозволяє оцінити рівномірність розподілу чисел у послідовності та визначити частоту повторення кожного символу;

– розподіл на площині застосовується для визначення залежностей між елементами послідовності;

– перевірка на монотонність допомагає визначити рівномірність шляхом аналізу незростаючих та неспадних підпослідовностей;

– перевірка серій виявляє області послідовних однакових або різних бітів, допомагає визначити рівномірність послідовності;

– автокореляційна функція використовується для оцінки кореляції між зсунутими копіями послідовностей та окремими підпослідовностями;

– графічний спектральний тест визначає структурні особливості в спектральному представленні послідовності;

– профіль лінійної складності допомагає визначити зміну складності послідовності та виявити аномалії.

Статистичні методи теж допомагають тестувати ГПВЧ. Статистичні властивості згенерованої послідовності визначаються числовими характеристиками. Ці методи базуються на оціночних критеріях, які дозволяють зробити висновки про те, наскільки послідовність подібна до випадкової. На відміну від графічних методів, де інтерпретація результатів може бути суб'єктивною через людський фактор, статистичні тести надають чисельні характеристики, які забезпечують однозначність висновків. Для проведення тестування на випадковість існує багато алгоритмів, серед яких відомі тести такі як NIST STS, Diehard, Crypt-X, тести Д. Кнута, FIPS, AIS та інші:

– тести Дональда Кнута [37] – одні з перших статистичних тестів і ґрунтуються вони на статистичному критерії хі-квадрат (критерій згоди Пірсона). Основна ідея полягає в порівнянні значень статистики хі-квадрат (що обчислюється для послідовності) з табличними результатами, які відомі для різних розподілів. Цей підхід дозволяє зробити висновок про те, наскільки добре випадкова послідовність відповідає деякому теоретичному розподілу. Один з найбільших плюсів тестів Кнута полягає в їхній відносно невеликій кількості та наявності швидких алгоритмів для їх виконання. Вони є важливим інструментом для перевірки генераторів псевдовипадкових чисел, особливо в контексті криптографії та інших додатків, де важлива випадковість. Проте, слід зазначити, що недоліком тестів Кнута є відсутність чіткого однозначного трактування результатів, що може потребувати додаткової аналізу та інтерпретації;

– diehard [38] вважається також одним з перших великих наборів тестів для оцінки криптографічної стійкості генераторів псевдовипадкових чисел. Diehard включає більше десяти різноманітних тестів, які оцінюють властивості послідовностей псевдовипадкових чисел з різних сторін. Ці тести перевіряють рівномірність розподілу, кореляцію, залежність між елементами послідовності, наявність послідовностей та інші статистичні характеристики. Він був важливим кроком у забезпеченні надійності генерації випадкових чисел. Diehard залишається важливим інструментом для випробування генераторів псевдовипадкових чисел, хоча на сьогоднішній день, через розвиток

криптографічних стандартів, з'явилися більш сучасні тести, наприклад такі як: NIST Statistical Test Suite;

– NIST Statistical Test Suite [22, 39] – це набір статистичних тестів, розроблений Національним інститутом стандартів і технологій (NIST) США. Він включає різноманітні тести, які перевіряють різні статистичні властивості послідовностей, такі як: рівномірність розподілу, автокореляція, апроксимація до рівномірного розподілу, виявлення структурних залежностей та багато інших.

Пакет NIST STS - це 15 статистичних тестів з:

1. The Frequency (Monobit) Test;
2. Frequency Test within a Block;
3. The Runs Test;
4. Tests for the Longest-Run-of-Ones in a Block;
5. The Binary Matrix Rank Test;
6. The Discrete Fourier Transform (Spectral) Test;
7. The Non-overlapping Template Matching Test;
8. The Overlapping Template Matching Test;
9. Maurer's "Universal Statistical" Test;
10. The Linear Complexity Test;
11. The Serial Test;
12. The Approximate Entropy Test;
13. The Cumulative Sums (Cusums) Test;
14. The Random Excursions Test;
15. The Random Excursions Variant Test.

NIST Statistical Test Suite є важливим інструментом для випробування ГПВЧ, а також для перевірки випадкових послідовностей, що використовуються в різних областях, де важливо мати надійний та криптографічно стійкий випадковий вихід.

Crypt-X – комерційний набір статистичних тестів, розроблений науково-дослідним центром інформаційної безпеки в Технологічному університеті Квінсленду. Цей набір тестів призначений для оцінки якості ГПВЧ і може використовуватися з різними типами алгоритмів генерації, включаючи як потокові, так і блокові шифри, а також генератори потоку ключів. У набір включені такі тести: частотний, на послідовність однакових бітів, лінійна складність, складність послідовності, двійкова похідна, зміна точки.

FIPS [40] – методика, що використовується для технологічного аналізу вихідних послідовностей ГПВЧ. Складається FIPS з чотирьох статистичних тестів: монобітний, «покер-тест», тест серій, тест довжини серій. Якщо будь-який з тестів не пройдений, то вважається, що генератор не пройшов весь комплекс перевірок.

AIS знаходить застосування як в процесі генерації послідовностей, так і в їх аналізі, а також при технологічних випробуваннях. Основна концепція AIS полягає в тому, що оцінка якості генераторів псевдовипадкових чисел має враховувати їхню відповідність криптографічним застосуванням, в яких вони використовуються. AIS складається з чотирьох функціональних класів: K1, K2, K3, K4. Кожен з них формулює ієрархічні вимоги до генераторів псевдовипадкових чисел. Аналіз показав, що методика AIS 31 продемонструвала подібні результати до відомого пакету тестування NIST STS з точки зору ефективності. Перевагою AIS 31 є можливість тестування в реальному часі, а також в процесі досліджень.

ВИСНОВКИ

Отже, генератори псевдовипадкових чисел відіграють невід'ємну роль у сучасному світі, де вони знаходять застосування в різних сферах. Потреба в якісних випадкових послідовностях стає все більшою в умовах зростаючого впливу цифрової технології. Важливість ГПВЧ полягає, зокрема, в їх внеску в забезпечення безпеки і конфіденційності в інформаційних системах. Однак зростання обчислювальної потужності та сучасні вимоги до криптографічної стійкості ставлять під сумнів ефективність і надійність деяких методів генерації псевдовипадкових чисел. Це створює необхідність постійного дослідження та вдосконалення ГПВЧ, зокрема розробки нових методів та вдосконалення існуючих для забезпечення відповідності сучасним стандартам безпеки.

Для отримання надійного висновку про придатність або непридатність ГПВЧ до використання в конкретних задачах необхідно використовувати комплексний підхід, включаючи декілька різних тестів. Це дозволяє збільшити достовірність оцінки, адже різні тести перевіряють різні аспекти.

ЛІТЕРАТУРА

[1] Gnatyuk, S., Y. Burmak, R. Berdibayev, M. Aleksander, D. Ospanova. «Метод побудови генераторів псевдовипадкових послідовностей для криптографічних застосувань у 5G мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», вип. 4, вип. 12, Червень 2021, С. 151-162.

[2] Горбенко, І. Д., Н. В. Шапочка, and О. О. Козулін. "Обґрунтування вимог до генераторів випадкових бітів згідно ISO/IEC 18031." Радіоелектронні і комп'ютерні системи 6. 2009. С. 94-97.

[3] Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. Харків.: Вид-во «Форт», 2012. 880 с.

[4] Євсеєв С.П., Корольов Р.В., Краснянська М.В.. Аналіз сучасних методів формування псевдовипадкових послідовностей. Восточно-Европейский журнал передовых технологий №3(45), 2010. С.11-15.

[5] Гарасимчук, О. І., Максимович, В. М. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості. Захист інформації, 5(3 (16)), 2002. С. 29-36.

[6] Mandrona, M.; Maksymovych, V.; Harasymchuk, O.; Kostiv, Y. Generator of pseudorandom bit sequence with increased cryptographic immunity. Metall. Min. Ind. 2014. pp. 24-28.

[7] Barker, E. , Feldman, L. and Witte, G. Recommendation for Random Number Generation Using Deterministic Random Bit Generators, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=919165 (Accessed November 20, 2022).

[8] L'Ecuyer, Pierre & Simard, Richard. TestU01: A C library for empirical testing of random number generators. ACM Transactions on Mathematical Software 33(4, article 22). 2007.

[9] Baldanzi, L.; Crocetti, L.; Falaschi, F.; Bertolucci, M.; Belli, J.; Fanucci, L.; Saponara, S. Cryptographically Secure Pseudo-Random Number Generator IP-Core Based on SHA2 Algorithm. Sensors 2020, 20, 1869. https://doi.org/10.3390/s20071869.

[10] Orúe, A.B., Hernández Encinas, L., Fernández, V., Montoya, F. (2018). A Review of Cryptographically Secure PRNGs in Constrained Devices for the IoT. In: Pérez García, H., Alfonso-Cendón, J., Sánchez González, L., Quintián, H., Corchado, E. (eds) International Joint Conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain, September 6-8, 2017. Proceeding. SOCO ICEUTE CISIS 2017 2017 2017. Advances in Intelligent Systems and Computing, vol 649. Springer, Cham. https://doi.org/10.1007/978-3-319-67180-2_65.

[11] Maksymovych, V.; Shabatura, M.; Harasymchuk, O.; Shevchuk, R.; Sawicki, P.; Zajac, T. Combined Pseudo-Random Sequence Generator for Cybersecurity. Sensors (Basel) 2022, 22, 9700, doi:10.3390/s22249700.

[12] Maksymovych, V.; Nyemkova, E.; Justice, C.; Shabatura, M.; Harasymchuk, O.; Lakh, Y.; Rusynko, M. Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators. Electronics (Basel) 2022, 11, 2039, doi:10.3390/electronics11132039.

[13] Maksymovych, V.; Shabatura, M.; Harasymchuk, O.; Karpinski, M.; Jancarczyk, D.; Sawicki, P. Development of Additive Fibonacci Generators with Improved Characteristics for Cybersecurity Needs. Appl. Sci. (Basel) 2022, 12, 1519, doi:10.3390 / app 1203-1519.

[14] Almaraz Luengo, E. A brief and understandable guide to pseudo-random number generators and specific models for security. Statistic Surveys, 2022. pp. 137-181.

[15] Поперешняк С.В.. Тестування генератора псевдовипадкових чисел як складова безпеки інтернету речей. «Наукоємні технології», № 2(46), 2020.

[16] Kietzmann, T. C. Schmidt, and M. Wählisch, A Guideline on Pseudorandom Number Generation (PRNG) in the IoT. ACM Comput. Surv. 2022, 54, 1–38. https://doi.org/10.1145/3453159.

[17] Orúe, A.B.; Hernández Encinas, L.; Fernández, V.; Montoya, F. A Review of Cryptographically Secure PRNGs in Constrained Devices for the IoT. In Proceedings of the SOCO 2017, ICEUTE 2017, CISIS 2017: International Joint Conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain, 6–8 September 2017; Pérez García, H., Alfonso-Cendón, J., Sánchez González, L., Quintián, H., Corchado, E., Eds.; (Advances in Intelligent Systems and Computing Book Series); Springer: Cham, Switzerland, 2018; Volume 649. https://doi.org/10. 1007/ 978-3-319-67180-2_65.

[18] A Comparative Study on Pseudo Random Number Generators in IoT devices. Efe Alkan. Delft University of Technology, Bachelor Seminar of Computer Science and Engineering, July, 2021.

[19] Lew, Chee Hon and Chaw-Seng Woo. "Design and Implementation of -Text based Watermarking combined with Pseudo-Random Number Generator (PRNG) for Cryptography Application.", 2013.

[20] Chen, J., Miyaji, A., Su, C. (2014). Distributed Pseudo-Random Number Generation and Its Application to Cloud Database. In: Huang, X., Zhou, J. (eds) Information Security Practice and Experience. ISPEC 2014. Lecture Notes in Computer Science, vol 8434. Springer, Cham. https://doi.org/10.1007/978-3-319-06320-1_28.

[21] De Bernardi, M., Khouzani, M.H.R., Malacaria, P. (2019). Pseudo-Random Number Generation Using Generative Adversarial Networks. In: et al. ECML PKDD 2018 Workshops. ECML PKDD 2018. Lecture Notes in Computer Science, vol 11329. Springer, Cham. https: // doi.org / 10.1007 /978-3-030-13453-2_15.

[22] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo. NIST Special Publication 800-22, Revision 1a, April, 2010.

[23] PAROL M., DĄBAL P, SZPLET R. Pseudo-random bit generators based on linear-feedbackshift registers in a programmable device. Measurement Automation Monitoring, Jun. 2016, no. 06, vol. 62, ISSN 2450-2855.

[24] R. S. Durga, C. K. Rashmika, O. N. V. Madhumitha, D. G. Suvetha, B. Tanmai and N. Mohankumar, "Design and Synthesis of LFSR based Random Number Generator," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 438-442, doi: 10.1109/ICSSIT48917.2020.9214240.

[25] Гарасимчук О.І., Максимович В.М., Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей // Вісник Національного університету "Львівська політехніка" "Комп'ютерні науки та інформаційні технології", №521, 2004. С. 17-23.

[26] Cryptography and Network Security: Principles and Practice, 7th edition. William Stallings.767 p.

[27] Sovyn Ya., Nakonechny Yu., Opirskyy I., Stakhiv M. Analysis of hardware support of cryptography in Internet of Things-devices // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1, pp. 36-48.

[28] Н.А. Кошева, Н.І. Мазниченко. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів. «Системи обробки інформації», №6(113), 2013.

[29] A Systematic Analysis of the Juniper Dual EC Incident. Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, Hovav Shacham. October, 2016.

[30] Добрецова О.А., Руснак М.А.. Генератор одноразових захищених чатів. Чернівецький національний університет імені Юрія Федьковича. 2022.

[31] Деркач Д.О. Обґрунтування методики захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках. Дніпро, 2020.

[32] Крюков К.Є.. Порівняльний аналіз криптографічно стійких генераторів псевдовипадкових чисел. VI Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", 2023.

[33] Соколовська, Г. В. Статистичний аналіз генераторів псевдовипадкової послідовності у програмних середовищах Matlab та Mathcad [Текст] / Г. В. Соколовська // Моделювання та інформаційні технології: зб. наукових праць. 2013. Вип. 66. С. 26-30.

[34] Поперешняк С.В. Методика статистичного аналізу випадковості послідовностей, що породжуються генераторами випадкових та псевдовипадкових чисел. Телекомунікаційні та інформаційні технології. 2022. № 3 (76).

[35] Lorek P.; Łoś G.; Gotfryd K.; Zagórski F. On testing pseudorandom generators via statistical tests based on the arcsine law. Journal of Computational and Applied Mathematics 2020, 380, 112968, doi:10.1016/j.cam.2020.112968.

[36] Sýs, M.; Říha, Z. Faster Randomness Testing with the NIST Statistical Test Suite. In Security, Privacy, and Applied Cryptography Engineering; Springer International Publishing: Cham, 2014; pp. 272-284 ISBN 9783319120591.

[37] Knuth, Donald E. The Art of Computer Programming. 3rd ed., Addison Wesley, 1997.

[38] 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). pp. 53-57.

[39] NIST SP 800-22 Version 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications; NIST: Gaithersburg, MD, USA, (2010); p. 131. Available online: https://nvlpubs.nist.gov / nistpubs / Legacy/SP/ nistspecialpublication800-22r1a.pdf (accessed on 20 April 2023).

[40] Min, Lequan et al. "Analysis of FIPS 140-2 Test and Chaos-Based Pseudorandom Number Generator.", 2013.

APPLICATION OF GENERATORS OF PSEUDO-RANDOM NUMBERS AND SEQUENCES IN CYBER SECURITY, METHODS OF THEIR CONSTRUCTION AND QUALITY ASSESSMENT

Due to the rapid development of computing and measurement technology, as well as the implementation of advanced technologies, the scope of application for pseudo-random number generators and pseudo-random sequences has significantly expanded, placing new demands on their design and quality evaluation methods. Quality pseudo-random sequences, although essentially deterministic, possess nearly all the properties of true random processes and successfully replace them, as the generation of random sequences is extremely complex. Due to the diversity and wide range of tasks that require the use of pseudo-random numerical sequences, new algorithms, methods, and tools for obtaining such sequences are constantly being developed and improved. Using pseudo-random sequence generators, one can obtain sequences of numbers where each element is practically independent of others and follows a specific prescribed distribution law, with the uniform distribution being the most common. Thanks to their statistical properties and generation speed, pseudo-random number and sequence generators are essential tools in various fields, including simulation modeling (economic, mathematical, physical, medical research, military applications), computer game development (generation of 3D models, textures, and worlds, as well as creating diversity and randomness in the behavior of characters and events), and measurement technology. Overall, it's important to note that developers of pseudo-random sequence generators face a set of stringent requirements regarding specific characteristics of the results they create using these generators. These requirements can vary depending on the generator's intended purpose and can be particularly high and demanding when pseudo-random sequences are used in cyber-security and information protection. For example, for cryptographic applications, the requirements are extremely rigorous and may sometimes even contradict each other. To verify whether the generated sequence meets the specified criteria and requirements, it is necessary to evaluate its quality, which involves assessing various features and parameters. Since the development of pseudo-random sequence generators aims to make them resemble sequences of truly random numbers, the basis for any evaluation of generators lies in comparing the statistical characteristics of the generated sequence with the characteristics of truly random sequences. For this purpose, various tests are used, which allow the detection of existing statistical regularities and, thus, the identification of low-quality pseudo-random sequences.

Keywords: pseudorandom number generators, pseudorandom sequence generators, cyber security, generation, testing, quality assessment.

Хомік Марія Анатоліївна, студентка 3-го курсу, спеціальності «Кібербезпека» Національного університету «Львівська політехніка».

Mariia Khomik, A third-year student the Department of Information Security, National University "Lviv Polytechnic".
E-mail: mariia.khomik.kb.2021@lpnu.ua.
Orcid ID: 0009-0004-6031-5618.

Гарасимчук Олег Ігорович, к.т.н., доцент, доцент кафедри захисту інформації Національного університету «Львівська політехніка».

Oleh Harasymchuk, Ph.D., Associate Professorat the Department of Information Security, National University "Lviv Polytechnic".
E-mail: oleh.i.harasymchuk@lpnu.ua.
Orcid ID: 0000-0002-8742-8872.

DOI: 10.18372/2410-7840.25.17941
УДК 004.056.5

МЕТОДОЛОГІЯ ОЦІНКИ СУМИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сергій Гончар, Олександр Потенко

Для визначення економічної доцільності застосування і вибору тих чи інших заходів по обробці ризику проекту у цілому, включаючи як організаційні, так і технічні, необхідно здійснити оціночне порівняння вартості таких заходів з максимальною величиною збитків в результаті дії декількох ризиків. В роботі запропонована методологія оцінки суми ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури. Запропонована у статті методологія базується на застосуванні методів розрахунку суми ризиків і обчислення комплексного ризику. На підставі запропонованої в даній статті методології представлено структурні рішення обчислювальних систем оцінки ризику кібербезпеки інформаційних систем, що реалізують методи