DOI: 10.18372/2410-7840.25.18222
УДК 004.056

АНАЛІЗ ЗАГРОЗ ДЛЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ І ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ТА ЗАХОДИ ЗАХИСТУ

Марія Хомік, Олег Гарасимчук

В сучасному цифровому світі з різноманітними застосуваннями, включаючи криптографію, кібербезпеку та захист даних, проблема побудови надійних та безпечних генераторів псевдовипадкових чисел та послідовностей набуває особливо актуального значення. Ці генератори створюють числові послідовності, які здаються випадковими, але насправді є детермінованими та мають певну структуру, що робить їх корисними для застосування у багатьох галузях. Зокрема вони використовуються для генерації секретних ключів, захисту конфіденційності, забезпечення цілісності даних та безпеки транзакцій, тому їх безпека є критичною для застосунків, які використовують такі генератори. Проте з ростом популярності та розширенням сфери застосування генераторів псевдовипадкових чисел та генераторів псевдовипадкових послідовностей зростає і рівень їх вразливості перед різними видами атак. Атаки на дані генератори можуть призвести до розкриття секретних параметрів та підриву систем безпеки. Зловмисники та хакери намагаються знайти різноманітні вразливості в методах та алгоритмах побудови таких генераторів, для часткового або повного розкриття принципів роботи генератора. В даній роботі га основі ґрунтовного аналізу наукових публікацій фахівців, які займаються розробкою, дослідженням, оцінкою якості та застосуванням генераторів псевдовипадкових чисел та генераторів псевдовипадкових послідовностей визначені та описані основні вразливості даних генераторів, класифіковані і описані види атак, визначений вплив цих атак на дані генератори та рекомендовані заходи безпеки, визначені стандарти та методи тестування для підвищення надійності, захисту таких генераторів та пом'якшення їх вразливостей.

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

ВСТУП

У сучасному світі, насиченому інформацією та науковими досягненнями в галузі цифрових технологій, генератори псевдовипадкових чисел (ГПВЧ), а також псевдовипадкових послідовностей (ГПВП) мають широкий спектр застосування: від імітаційного моделювання у економічній, військовій та інших областях до застосування для генерації секретних ключів у сфері криптографії та забезпечення цілісності фінансових транзакцій і даних у банківському секторі, де виступають вирішальними складовими для забезпечення захисту цінних даних. З їхньою допомогою створюються послідовності чисел, які, з одного боку, мають властивості випадковості, а з іншого – є детермінованими, що робить їх незамінними для широкого спектру застосувань в різних сферах [1-5]. Варто зазначити, що ГПВЧ та ГПВП відіграють ключову роль у забезпеченні конфіденційності та безпеки інформації.

Проте із зростанням популярності ГПВЧ та ГПВП збільшується і рівень їхньої вразливості перед різноманітними атаками. Особливо це відчувається, коли дані генератори використовуються у сферах з підвищеними вимогами до їх якості, зокрема для вирішення задач кібербезпеки.

Вимоги до безпеки цих генераторів стають дедалі важливішими, оскільки атаки на них можуть призвести до серйозних наслідків: від порушення конфіденційності та витоку цінних даних до підриву криптографічних систем та загроз приватності користувачів. Необхідно зазначити також, що атаки на ГПВЧ та ГПВП стають дедалі виразнішими та складнішими. Кіберзлочинці та хакери активно використовують різні методи та підходи для зламу генераторів псевдовипадкових послідовностей.

Зважаючи на це, запобігання таким атакам, усунення можливих вразливостей стає невід'ємною частиною сучасних методів, способів та алгоритмів генерування псевдовипадкових чисел та послідовностей. Виробники та дослідники активно працюють над розробкою та впровадженням передових методів захисту для забезпечення безпеки

ГПВЧ та ГПВП, що стає пріоритетом для організацій та індивідів, які використовують такі генератори.

Загалом, розуміння сутності атак і їхніх наслідків має вирішальне значення для розвитку ефективних стратегій захисту та забезпечення безпеки в сучасному інформаційному середовищі.

Українські та іноземні науковці активно працюють над питаннями дослідження методів та способів побудови ГПВЧ та ГПВП, дослідженню їх вразливостей, аналізу проблем їх безпеки, а також можливим атакам на дані генератори [6-10]. Аналізуючи їх праці можна побачити, наскільки важливою є надійність та безпека генератора псевдовипадкових чисел/послідовностей у різних сферах застосування, які бувають атаки та як може себе поводити зловмисник при недостатньому захисті ГПВЧ чи ГПВП.

Останнім часом спостерігається різке зростання потреби у використанні якісних та надійних ГПВЧ та ГПВП, зокрема для:

– криптографічних застосувань, де ГПВЧ та ГПВП використовуються для генерації ключів і векторів ініціалізації в криптографії. Якщо такі генератори не будуть безпечними, то це може призвести до порушення конфіденційності, цілісності та доступності даних;

– комп'ютерної безпеки, коли багато програм та систем використовують псевдовипадкові числа для генерації токенів, паролів та ідентифікаторів. Якщо такі числа зловмисник зможе передбачити, то це створює потенційну вразливість для атак і несанкціонованого доступу;

– інформаційної безпеки, коли такі генератори використовуються для забезпечення безпеки даних у багатьох областях, таких як банківська справа, медицина, оборона тощо, де зберігається чутлива інформація, в разі порушення якої може виникнути серйозна загроза;

– контролю доступу, коли відбувається генерування токенів і ключів доступу. Якщо ГПВЧ чи ГПВП не буде безпечним, то це може призвести до несанкціонованого доступу до систем та ресурсів;

– інтернету речей (IoT), коли багато пристроїв, що використовують псевдовипадкові числа чи послідовності підключено до Інтернету, безпека генерації випадкових чисел стає ще важливішою. Вразливість в цій області може мати серйозні наслідки для пристроїв і мереж IoT;

– криптографічних протоколів, деякі з яких (наприклад SSL/TLS) для шифрування з'єднань у мережі, використовують псевдовипадкові числа для створення сеансових ключів. Якщо ці псевдовипадкові числа можна передбачити або ж підробити, то це може призвести до злому з'єднань і розкриття конфіденційної інформації;

– забезпечення довгострокової безпеки для криптовалюти чи при довгостроковому зберіганню даних, коли безпека таких генераторів повинна гарантуватися на тривалий термін. Вразливості в ГПВЧ можуть привести до втрати доступу до активів або конфіденційності даних у майбутньому.

Наведені вище фактори підкреслюють важливість безпеки ГПВЧ та ГПВБ у цифровому світі. Забезпечення надійності та криптографічної безпеки цих генераторів є обов'язковим завданням для захисту даних, довіри користувачів та забезпечення нормального функціонування багатьох систем і додатків.

Варто зазначити, що зі зростанням потреби у таких генераторах збільшується і кількість атак на них. Наприклад, в [6] акцентується увага на безпеці ГПВЧ в контексті сучасних технологій переносних пристроїв, електроніки та мікроелектронних систем, де обмеженість джерел ентропії може бути серйозним викликом.

Достатня кількість досліджень зосереджена на спробах вдосконалити систему надійності ГПВЧ та ГПВП шляхом створення нових механізмів генерації.

Зокрема у [7] пропонується механізм генерації псевдовипадкових чисел з високим рівнем випадковості. Його дизайн базується на геометричних структурах, що імітуються програмно, зокрема, на обертальних циліндрах, які активуються також за допомогою випадкових входів, що створюються на основі подій електронної системи, на якій він працює. Завдяки високому рівню випадковості його виходи можуть бути використані для створення надійних систем захисту даних.

Робота [8] демонструє нам гібридний метод генерації псевдовипадкових чисел, використовуючи лінійний зріст зсуву (LFSR) та лінійний конгруентний генератор (LCG). Такий метод для

генерації ключів об'єднує дві технології, які генерують нові послідовності чисел великого обсягу. Забезпечується вищий рівень конфіденційності завдяки поєднанню внутрішніх чисел, згенерованих за допомогою LFSR, з LCG (з використанням коренів у нелінійних ітераційних циклах). У цьому гібридному підході вдається уникнути передбачуваності, яка притаманна лінійним структурам LCG і LFSR, і досягти високої випадковості. Результати оцінки якості свідчать про успішне проходження тестів та стійкість до атак методами грубої сили і диференційної атаки.

Також у [10] пропонується схема генерації псевдовипадкових послідовностей на основі карт Комперца та кускового відображення. Результати показали, що послідовності, створені цією схемою, мають високий рівень випадковості та можуть бути використані для створення псевдовипадкових чисел та секретних ключів. Секретні ключі, згенеровані цією схемою, вважаються відносно стійкими до атак.

Загалом аналіз проблеми побудови ГПВЧ та ГПВП показав, що завдання дослідження важливості безпеки цих генераторів та аналіз можливих атак на них вкрай актуальне. У сучасному світі, де дедалі більше сфер діяльності використовують криптографічні рішення, забезпечення надійності ГПВЧ та ГПВП має стратегічне значення для забезпечення безпеки даних і інформаційних процесів у різних галузях.

Основна мета дослідження полягає в аналізі проблем безпеки генераторів псевдовипадкових чисел та псевдовипадкових послідовностей. Для цього необхідно визначити основні вразливості та головні причини, види і наслідки успішних атак на ГПВЧ та ГПВП, а також розглянути заходи безпеки, необхідні для їхнього правильного і безпечного функціонування. Для досягнення даної мети необхідно проаналізувати вимоги до характеристик таких генераторів і типи атак шляхом опрацювання останніх публікацій і досліджень, розробити класифікацію на основі такого аналізу. Отримані результати можуть бути корисними та стати цінним джерелом інформації і рекомендацій для тих, хто працює у галузі кібербезпеки та займається діяльністю, яка вимагає використання псевдовипадкових чисел та відповідних генераторів.

ОСНОВНА ЧАСТИНА

Основні вразливості та причини здійснення успішних атак на ГПВЧ та ГПВП

ГПВЧ та ГПВП можуть мати різні слабкі місця і вразливостей, якими можуть скористатися зловмисники. Серед найбільш поширених вразливостей можна виділити:

– недостатня ентропія. ГПВЧ та ГПВП часто залежать від початкового значення, яке повинно мати достатню ентропію (непередбачуваність), щоб забезпечити випадковість. Якщо джерело ентропії є слабким або передбачуваним, згенеровані числа/послідовності можуть бути не зовсім випадковими, що робить систему вразливою до передбачуваності;

– погане керування початковим кодом. Якщо керування початковим числом, яке використовується для ініціалізації генератора, буде обрано погано або не буде безпечним, зловмисники можуть вгадати або отримати початкове число, тим самим підриваючи безпеку генератора;

– слабкі алгоритми. Окремі ГПВЧ та ГПВП використовують слабкі або застарілі алгоритми, які мають відомі вразливості. Наприклад, лінійний конгруентний генератор (LCG) є класичним прикладом алгоритму з відомими недоліками;

– невипадковість. ГПВП повинні виробляти послідовності, які виглядають випадковими і для яких не спостерігаються помітні шаблони або упередження. Генератори, які створюють вихідні дані з характеристиками, що не наближені до випадкових є вразливими до статистичного аналізу та атак;

– слабкість криптографії. Псевдовипадкові генератори, які використовуються в криптографічних програмах, повинні бути розроблені, щоб протистояти різним типам атак, включаючи атаки з прогнозуванням і криптоаналіз. Слабкі або криптографічно незахищені генератори можуть бути вразливими для експлуатації і не надавати необхідних гарантій безпеки;

– відсутність джерел ентропії. Псевдовипадкові генератори, які не мають доступу до різноманітних джерел ентропії, можуть бути вразливими. Джерела ентропії, такі як апаратні генератори випадкових чисел, підвищують безпеку згенерованих послідовностей;

– ненадійні алгоритми. Використання слабких або застарілих алгоритмів ГПВЧ та ГПВП може

призвести до проблем із безпекою. Багато старих ГПВЧ, як-от лінійний конгруентний генератор (LCG), мають відомі вразливості, тому їх слід уникати на користь сучасних криптографічно захищених альтернатив;

– погане тестування. Псевдовипадкові генератори повинні пройти ретельне тестування та аналіз за допомогою відомих пактів тестів, щоб виявити вразливі та слабкі місця. Погане тестування може призвести до того, що проблеми безпеки залишаться невиявленими.

Щоб пом'якшити наведені вразливості, дуже важливо використовувати добре розроблені, криптографічно захищені генератори псевдовипадкових подій і дотримуватися найкращих практик щодо їх впровадження та оцінки їх якості. Крім того, поєднання генераторів псевдовипадкових чисел з апаратними генераторами випадкових чисел може покращити безпеку генерації випадкових чисел у критично важливих програмах. Регулярний аудит і оновлення генераторів також є важливими для усунення будь-яких нововиявлених вразливостей. Також важливо зберігати початкове значення в секреті та використовувати сильні, непередбачувані джерела ентропії під час ініціалізації ГПВЧ чи ГПВП для критично важливих для безпеки завдань.

Атака на ГПВЧ/ГПВП спрямована на розкриття секретних параметрів, що використовуються для генерування псевдовипадкових чисел/послідовностей, з метою подальшого передбачення або вгадування значень цих чисел/послідовностей. В результаті проведення атаки зловмисником можливе повне або часткове розкриття генератора.

Повне розкриття – це вдало реалізована атака, в результаті якої противнику стають відомі секретні параметри генератора, за допомогою яких відновлюється вся вихідна послідовність генератора.

Часткове розкриття – це вдало реалізована атака, в результаті якої противник дізнається частину інформації про генератор і може отримати (або з великою ймовірністю передбачити) частину вихідної послідовності.

Атаку можна характеризувати ймовірністю успіху її проведення, середнім (максимальним) часом та обсягом пам'яті, необхідним для її реалізації, обсягом додаткової необхідної інформації (біти ключа, додаткові входи тощо).

Здійснення успішних атак на генератори псевдовипадкових чисел та послідовностей може мати безліч потенційних причин, які варто вивчити і враховувати для забезпечення безпеки та надійності цих систем. Основні з них, які частіше призводять до серйозних наслідків та сприяють зловмисникам можна виокремити в наступному вигляді (рис. 1).

Рис. 1. Основні причини здійснення успішних атак на ГПВЧ та ГПВП

Доведено, що послідовність є псевдовипадковою тоді і лише тоді, коли вона непередбачувана, тобто витримує тестування черговим бітом. Тому перша причина успішної атаки – передбачуваність. Математик Берлекамп-Мессі [11] виявив, що будь-який ГПВЧ, заснований на відомому математичному алгоритмі та зворотному зв'язку, може бути передбаченим. Конкретніше, для даного N-бітового ГПВЧ з невідомим поліномом зворотного зв'язку достатньо 2N біт для того, щоб передбачити значення наступного біта. Ця прозорість внутрішньої структури ГПВЧ використовується зловмисниками для відновлення послідовності, що генерується.

Недостатньо великий період – друга з ключових проблем, з якою стикаються при використанні ГПВЧ та ГПВП [12]. Період – це кількість чисел або бітів, які можуть бути згенеровані ГПВЧ, перш ніж послідовність повториться. Основною проблемою короткого періоду ГПВЧ є те, що він зменшує кількість можливих варіантів для генерації псевдовипадкових чисел. Коли зловмисник, який атакує знає, що період обмежений, він може використовувати це для передбачення насіння та

майбутніх згенерованих значень і таким чином відгадати всю послідовність. Зміщення в ГПВЧ та ГПВП відбувається тоді, коли певні числа або значення в генерованій послідовності виявляються більш чи менш ймовірними ніж інші. В такому випадку створюється нерівномірний розподіл, що може бути використаний у різних атаках. Дослідження, проведені Полом Пічем [13], підтвердили, що будь-який ГПВЧ, побудований на математичних формулах, міститиме певні патерни і періодичності, які діють як обмеження на їхню варіабельність. Секретність насіння є центральним елементом безпеки ГПВЧ та ГПВП, і атаки на цей параметр можуть мати серйозні наслідки для систем, що використовують такі генератори.

Якщо процес генерації насіння недостатньо випадковий або має системні вразливості, це може призвести до передбачуваності насіння та послідовностей чисел, що генеруються [14].

Зловмисники можуть аналізувати також швидкодію ГПВЧ та використовувати атаки, що базуються на часі [11].

Якщо ГПВЧ генерує числа надто повільно, атакуючі можуть намагатися визначити наступне значення, спираючись на час, який пройшов між генерацією попереднього та поточного числа.

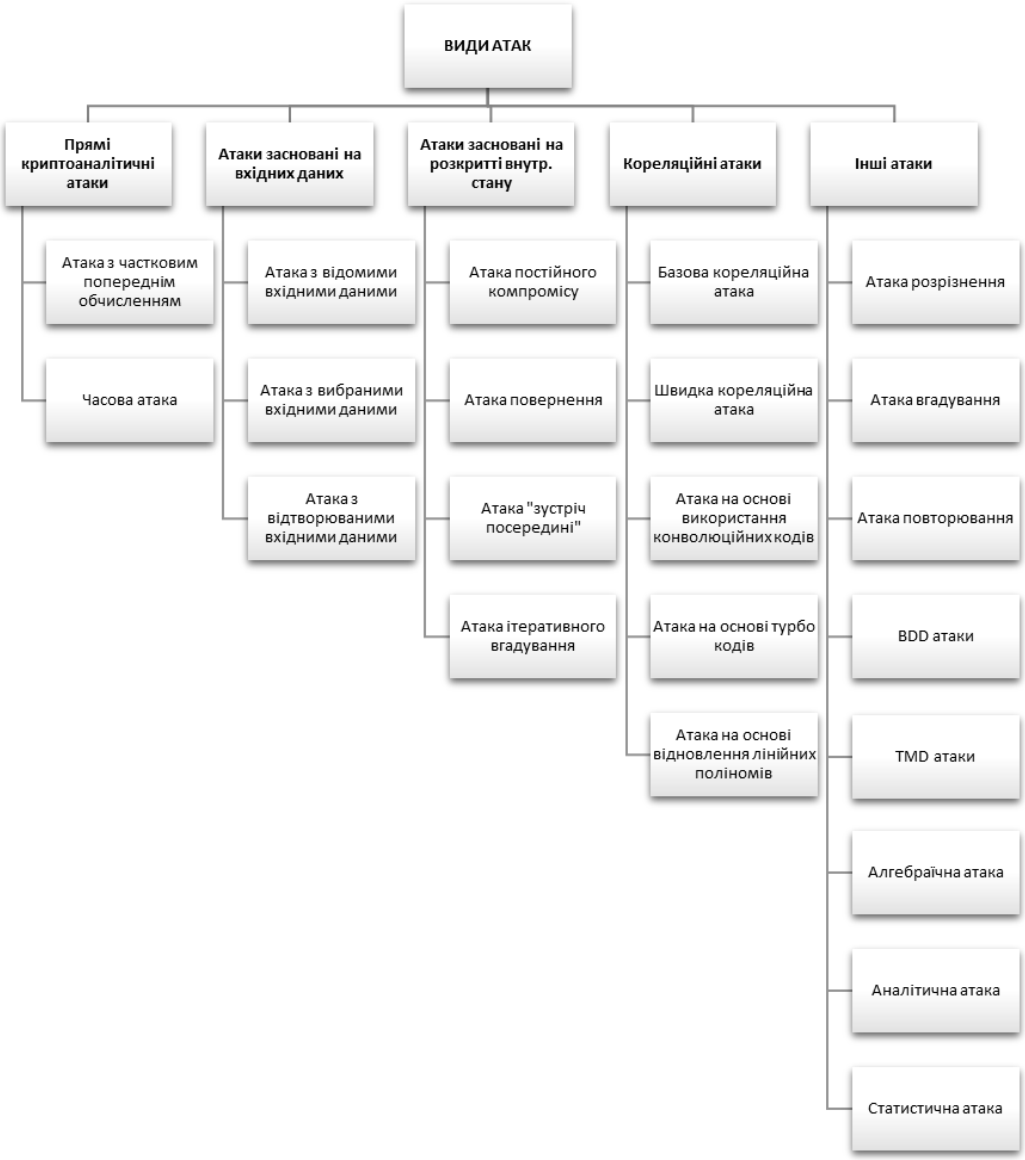

Рис. 2. Класифікація атак на ГПВЧ та ГПВП

Кожна з цих вразливостей може допомогти зловмиснику розробити атаки, спрямовані на обхід систем безпеки, та використовувати ці недоліки для досягнення своїх цілей. Забезпечення надійності та безпеки генераторів псевдовипадкових чисел полягає у врахуванні наведених вище основних причин реалізації таких атак. В такому випадку успішним атакам на ГПВЧ та ГПВП можна запобігти, а зловмисникам буде надзвичайно важко досягнути їхньої мети.

Види атак і їх вплив на ГПВЧ та ГПВП

В сучасному світі, де вірогідність атак на цифрові системи постійно зростає, розуміння різних видів атак на генератори псевдовипадкових чисел та псевдовипадкових послідовностей стає критично важливим для забезпечення кібербезпеки [11, 15-28]. Атаки на ГПВЧ можуть призвести до розкриття конфіденційної інформації, порушення інтегритету даних або навіть до псування криптографічних систем. Пропонуємо наступну класифікацію видів атак на генератори псевдовипадкових чисел та псевдовипадкових послідовностей (рис. 2).

Якщо зловмисник має можливість активно відстежувати вихідні дані генератора псевдовипадкових чисел та аналізувати закономірності їхнього виникнення, то це пряма криптоаналітична атака [16]. Цей вид атаки потенційно застосовний до більшості алгоритмів, які використовують ГПВЧ та ГПВП. У разі успішної прямої криптоаналітичної атаки зловмисник може визначити, як саме працює генератор та, можливо, встановити ключові параметри або знайти слабкі сторони в системі шифрування.

Існує два підвиди такої атаки:

1. Атака з частковим попереднім обчисленням застосовується до генераторів, які використовують лічильник. Зловмисник обирає певну кількість послідовних вихідних значень, t, які він очікує побачити, і обчислює хеш-суму для кожного t-го можливого значення лічильника [17]. Зловмисник має гарантію, що побачить одну з цих хеш-сум після t вихідних значень, і на цей момент він вже знає весь лічильник. Ця атака є непрактичною для 128-бітного лічильника, але вона встановлює верхню межу міцності такого генератора. З 232 вихідними значеннями зловмиснику знадобиться зробити 296 попередніх обчислень для здійснення атаки, а з 248 вихідними значеннями він мусив би зробити 280 попередніх обчислень. Ці атаки також потребують великої кількості пам'яті, але можливість обміну часу та пам'яті може скоротити цю вимогу до неї;

2. Часова атака – це використовування інформації про час, необхідний для виконання операцій або обчислень, щоб отримати конфіденційні дані або підірвати безпеку системи. Той, хто має можливість спостерігати за часом, необхідним для генерації кожного нового вихідного значення, може визначити, скільки нульових байтів знаходиться у лічильнику після кожної операції інкрементації. Це базується на кількості байтових додавань, які необхідно виконати для коректного збільшення лічильника. Варто зазначити, що атака має два аспекти [17]. По-перше, лічильники, які мають нульові байти у менш значущих розрядах, виливають через часовий канал значну кількість інформації, і таку ситуацію можна розглядати як «слабкий стан». По-друге, коли цю атаку комбінувати із атакою часткового попереднього обчислення, яка обговорювалася раніше, інформацію про час можна використовувати для визначення моменту, коли варто перевіряти вихід генератора щодо попередньо обчисленої таблиці. Хоча ця перевага є невеликою, вона все ж може бути використана зловмисником.

Якщо хтось використовує спеціально створені вхідні дані або вектори для вторгнення в безпеку ГПВЧ, то це атака заснована на вхідних даних. Її можна поділити на [19]:

1. Атаки з відомими вхідними даними – це вид атак, під час якого зловмисник може спостерігати частину вхідних даних, не маючи можливості їх змінити. Знання цих вхідних даних може бути використано для обмеження можливих варіантів вихідних даних, що, в свою чергу, знижує надійність генератора псевдовипадкових чисел. Такий вид атак може виникнути, коли оцінка ентропії вхідних даних є неточною. В цьому випадку зібрана ентропія містить менше випадковості, ніж користувач може спочатку припустити, і зловмисник може визначити певну частину вхідних даних. Додатково, атаки з відомими вхідними даними можуть бути успішними, якщо в якості вхідних даних використовуються спостережувані дані користувача, такі як вхідні, які передаються через мережу.

В цьому випадку зловмисник може використовувати знання про них для обчислення або обмеження можливих вихідних значень, що зробить генератор менш надійним;

2. Атаки з вибраними вхідними даними являють собою специфічний клас атак, де зловмиснику вже надається можливість контролювати та маніпулювати вхідними даними генератора. Він може намагатися швидко вивести генератор із стану або змусити його повторно генерувати певні послідовності. Це може призвести до порушення випадковості та передбачуваності вихідних даних генератора;

3. Атаки з відтворюваними вхідними даними схожі до попередніх, але не на стільки ефективні. Це атаки повторення вхідних даних. У цьому випадку зловмисник може відтворювати існуючі вхідні дані, але не може змінювати їх довільно.

Атаки на ГПВЧ, засновані на розкритті внутрішнього стану, передбачають ситуацію, де зловмисник вже має певну інформацію про внутрішній стан генератора псевдовипадкових чисел. Ці атаки спрямовані на розширення знань про стан генератора у різні моменти часу і на отримання доступу до попередніх або майбутніх вихідних значень. Така ситуація може виникнути, якщо процес генерації був розділений або якщо ГПВЧ був запущений в незахищеному стані. Генератори, які мають фіксоване початкове значення або повністю покладаються на обробку вхідних даних, можуть бути особливо вразливими до цих атак. У таких ситуаціях внутрішній стан може розкриватися, якщо він потрапляє на незахищену область жорсткого диска або через інші методи обміну даними.

Можна виділити чотири підвиди атак, заснованих на розкритті внутрішнього стану [19, 21]:

1. Атаки постійного компромісу, відомі також як «Permanent Compromise Attacks», відзначаються тим, що, якщо зловмисник отримав доступ до внутрішнього стану генератора S у певний момент часу t, то всі майбутні та минулі значення S в цьому генераторі стають вразливими до атаки. Це означає, що зловмисник може передбачати та контролювати всі значення S після t, а також використовувати цю інформацію для підірвання безпеки системи;

2. Атаки повернення чи «Backtracking Attacks» використовують компрометацію стану ГПВЧ S в певний момент часу t для визначення попередніх вихідних значень ГПВЧ. Така атака може бути особливо ефективною, оскільки, розкривши один стан генератора, зловмисник може визначити значення, які генератор створював у минулому. Це може призвести до розкриття важливої інформації, яку генератор використовував для шифрування або інших критичних операцій;

3. Атаки ітеративного вгадування або «Iterative Guessing Attack» використовують знання стану S в момент часу t та інтервенцію в проміжні вихідні дані генератора псевдовипадкових чисел для визначення стану S в момент часу $t + \varepsilon$ (ε – часова різниця між моментами часу "t" і "$t + \varepsilon$", показує, що зловмисник намагається визначити стан генератора в дуже близький час до моменту часу "t"), коли вхідні дані, зібрані протягом цього періоду часу, доступні для вгадування, але не відомі зловмиснику;

4. Атаки «зустріч посередині» суттєво поєднують в собі методи ітеративної атаки та атаки на повернення. Знання стану генератора S в моменти часу t та $t + 2\varepsilon$ дозволяє зловмиснику відновити стан S в момент часу $t + \varepsilon$. Ця атака полягає в тому, що зловмисник використовує інформацію про стан генератора у два різних моменти часу та намагається відновити стан на проміжному кроці часу, коли він знає частину вхідних даних, зібраних за цей період, але їх не знає повністю.

Потрібно виділити наступний вид атак на ГПВЧ та ГПВП – кореляційні атаки [19-21]. Вони використовують статистичний аналіз для знаходження зв'язків і кореляцій між вихідними значеннями генератора та вхідними параметрами, такими як ключі або інші величини, що впливають на генерацію. До кореляціних атак відносяться:

– базові кореляційні атаки;

– швидкі кореляційні атаки;

– атаки на основі використання конволюційних кодів;

– атаки на основі турбо кодів;

– атаки на основі відновлення лінійних поліномів.

Основна ідея базових кореляційних атак полягає в аналізі вихідних бітів ГПВЧ, які визначаються за допомогою лінійних регістрів зі зсувом. У таких регістрах біти зсуваються на одну або декілька позицій, і новий біт обчислюється як лі-

нійна комбінація попередніх бітів. Кореляційні атаки спрямовані на виявлення статистичних залежностей між цими бітами. Наприклад, якщо два біти вихідної послідовності мають однаковий зсув, а вони сильно залежать один від одного, то зловмисник може використовувати цю кореляцію для прогнозування одного біта на основі іншого. Це може призвести до розкриття ключів і параметрів, які використовуються в генераторі.

Швидкі кореляційні атаки відрізняються своєю високою ефективністю та здатністю знаходити кореляції між вихідними бітами ГПВЧ відносно швидко.

Існують алгоритми з поліноміальним і експоненційним часом. Перші – це алгоритми, які працюють настільки ефективно, що час їхньої роботи залежить від розміру вхідних даних у вигляді поліноміальної функції. Іншими словами, час виконання цих алгоритмів зростає помірно зі збільшенням обсягу обчислень. Другі – це алгоритми, час виконання яких зростає експоненційно зі збільшенням розміру вхідних даних. Це означає, що такі алгоритми можуть стати дуже повільними при обробці великих обсягів даних [28].

Головна мета атак на основі використання конволюційних кодів полягає в тому, щоб знайти слабкі сторони у кодах, що використовуються та вимкнути їхню функцію виявлення або корекції помилок. Це може бути зроблено шляхом спеціального впливу на передавач, введення шуму, змінюючи параметри каналу, чи знайдення вразливостей у конкретних реалізаціях конволюційних кодів.

Атаки на основі турбо кодів – це спроби атакувати системи, які використовують турбо коди для передачі даних [26]. Однією з найреволюційніших ідей в теорії кодування стало впровадження турбо-кодів. Оригінальний турбо-код складається з двох конволюційних кодів, де інформаційні біти безпосередньо подаються в один з них, і переплетена версія тих самих інформаційних бітів подається в інший конволюційний код. Атаки на них можуть бути спрямовані на різні аспекти, такі як процес кодування, декодування чи витік конфіденційної інформації через вимірювання та аналіз випромінювання сигналу.

Атаки на основі відновлення лінійних поліномів – це атаки, спрямовані на розкриття параметрів лінійного полінома, що використовується в криптосистемі [24]. Вони відрізняються від інших, оскільки їх мета – розкриття структури полінома, а не обхід системи захисту. За межами вже згаданих атак на ГПВЧ та ГПВП існує розмаїття інших важливих видів.

Якщо зловмисник намагається визначити, чи вихідна послідовність, згенерована псевдовипадковим генератором, відрізняється від повністю випадкової послідовності, то це атака на розрізнення [18]. Основною характеристикою таких атак є час їх виконання (позначений як T) та ймовірність успіху (#). Атака на розрізнення вважається успішною, якщо вона може виділити відмінності між псевдовипадковою послідовністю та випадковою з ймовірністю не менше #. Важливо також відзначити, що подібна атака не завжди повинна розкривати секретний ключ чи початковий стан генератора. Наприклад, у випадку, коли псевдовипадкова послідовність має нерівну кількість нулів і одиниць, атака може просто виводити більшість бітів послідовності, визначаючи її властивості без розкриття конкретних ключів чи початкового стану генератора.

Атаки вгадування в контексті ГПВЧ та ГПВП також займають особливе місце [20]. Вони включають проведення "грубої сили", шукаючи секретний ключ чи початковий стан генератора. Цей вид атаки полягає в послідовному вгадуванні всіх можливих комбінацій l бітів внутрішнього стану генератора. Для кожного варіанту, зловмисник використовує генератор для генерації l бітів вихідної послідовності та порівнює їх із відомою вихідною послідовністю. Якщо хоча б один біт у вихідній послідовності відрізняється від відомої, то варіант вгадування вважається неправильним і відкидається. В іншому випадку, він додається до множини кандидатів на ключ. Для надійних генераторів, які успішно проходять стандартні статистичні тести, кількість неправильних варіантів в цьому наборі має бути дуже близькою до нуля, якщо кількість доступних бітів вихідної послідовності велика. У випадку, якщо існує більше одного кандидата на ключ, правильний ключ визначається, запускаючи генератор для розшифровки всіх повідомлень. Важливо відзначити, що атака на вгадування не обов'язково повинна відновлювати внутрішній стан генератора повністю. Той, хто здій-

снює атаку, може обмежитися частиною стану, спробуючи вивчити якнайбільше інформації та продовжити її.

Атаки повторювання – ще один вид, який варто виокремити в даній класифікації [21]. Їх суть полягає в тому, що злочинці перехоплюють вже відправлені дані або повідомлення і намагаються надіслати їх знову. Це може призвести до небажаних наслідків, таких як несанкціонований доступ до системи або обхід аутентифікації.

Атаки на основі бінарних схем прийняття рішень, відомі як BDD-атаки [20], є методами аналізу криптографічних систем, що використовують бінарні діаграми схем прийняття рішень для ефективного взлому ГПВЧ та ГПВП. Основна мета BDD-атаки полягає в знаходженні секретного ключа – k для ГПВЧ – G на основі відомого фрагмента ключової послідовності z, при умові, що ця послідовність була згенерована ГПВЧ – G за допомогою ключа k. Для досягнення цієї мети атака концентрується на пошуку мінімальної бінарної діаграми, D, яка представляє внутрішній стан ГПВЧ, так щоб виконувалося співвідношення z = G(k). Якщо довжина фрагмента z практично дорівнює довжині внутрішнього стану генератора псевдовипадкових чисел, то ключ k може бути відновлений з використанням діаграми D. Важливою умовою для ефективного застосування BDD-атак є те, що кожен біт ключової послідовності z повинен бути обчисленим як функція від відповідних бітів початкового стану генератора, згідно з нелінійним перетворенням або функцією стиску, підконтрольним криптографічним вимогам стійкості.

Атаки з урахуванням компромісу між часом, пам'яттю та даними (Time-Memory-Data Tradeoff, TMD) являють собою ефективний метод атаки на ГПВЧ та ГПВП [20]. Замість того, щоб використовувати повний перебір ключового простору, який вимагає значних обчислювальних зусиль, зловмисник обирає певну частину ключового простору для аналізу, знижуючи тим самим обсяг необхідних обчислень. Суть TMD атаки полягає в тому, що заздалегідь зловмисник генерує значення, які відповідають різним ключам з вибраної підмножини ключового простору. Для кожного такого ключа він обчислює вихідний рядок, який генерується цим ключем. Під час реальної атаки, коли зловмисник отримує певну кількість вихідних даних від захищеного генератора псевдовипадкових чисел, він порівнює отримані значення зі заздалегідь підготовленими. Якщо виявляє, що одне зі значень, які підготував заздалегідь, збігається з отриманими даними, це вказує на те, що відповідний ключ шифрування є частиною ключа. Зловмисник може використовувати цей ключ для отримання доступу до зашифрованих даних або для аналізу шифру. Ефективність такої атаки залежить від кількості вихідних даних, доступних для зловмисника. Чим більше вихідних даних він може отримати, тим вища ймовірність успіху цієї атаки.

Алгебраїчні атаки становлять серйозну загрозу безпеці ГПВЧ та вимагають заходів для захисту від них [20-21]. Ідея таких атак полягає в підборі системи алгебраїчних рівнянь, що описують залежність між бітами внутрішнього стану генератора і бітами ключового потоку, та їх подальшому розв'язанні. Алгебраїчні атаки складаються з трьох основних етапів. Перший етап передбачає підготовку системи алгебраїчних рівнянь до отримання ключової послідовності. Другий та третій етапи виконуються при відомому ключовому потоці, де зловмисник підставляє послідовні біти ключового потоку в підготовлену систему рівнянь та розв'язує її. При наявності достатньої кількості спостережень система рівнянь має невисокий алгебраїчний ступінь, що дозволяє вирішувати її за допомогою лінеаризації, наприклад методом Гаусса. Складність алгебраїчних атак залежить від ступеня рівнянь, і для зменшення цієї складності були запропоновані швидкі алгебраїчні атаки.

Існують ще два окремі види атак на ГПВЧ та ГПВП: аналітичні та статистичні [21]. Якщо аналітичні атаки спрямовані на розкриття алгоритмів та структур генераторів, статистичні атаки зазвичай виявляють відхилення від ідеалізованого випадкового розподілу. Поєднуючи ці два підходи, зловмисники можуть ефективно здійснювати атаки на генератори псевдовипадкових послідовностей та порушувати їх безпеку.

Загалом, існує велика кількість різних видів атак на генератори псевдовипадкових послідовностей. Кожен тип має власний набір методів та підходів для порушення безпеки ГПВЧ. Зловмисники можуть використовувати різні комбінації атак для досягнення своїх цілей, тому розробники

генераторів повинні приділяти значну увагу захисту та ретельно захищати свої системи.

Заходи захисту ГПВЧ та ГПВП

Безпека генераторів псевдовипадкових чисел є критично важливою для багатьох сфер інформаційних технологій. Недостатньо надійні або слабкі ГПВЧ та ГПВП можуть призвести до серйозних наслідків.

Запорукою безпеки генераторів псевдовипадкових послідовностей насамперед є дотримання міжнародних стандартів. Серед них варто виділити:

– міжнародний стандарт ISO/IEC 18031:2011 Information technology – Security techniques – Random bit generation [29], який визначає алгоритми генерування псевдовипадкових і випадкових чисел та встановлює статистичні тести для перевірки якості генераторів;

– міжнародний стандарт ISO/IEC 18032:2020 Information security – Prime number generation [30], який визначає методи генерування простих чисел і методи тестування чисел на простоту;

– національний стандарт ДСТУ ISO / IEC 19790:2015 Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів (ISO/IEC 19790:2012, IDT) [31].

Додаткові вимоги до алгоритмів та реалізацій методів і засобів генерування і тестування послідовностей псевдовипадкових чисел встановлюються також іншими стандартами. Серед них важливі [32-33] FIPS 140-3, ANSI X9.17, ANSI X9.31, ANSI X9.44, рекомендації NIST, зокрема NIST SP 800-22, та рекомендації від німецького органу зі стандартизації, такі як AIS-20 та AIS-31, і багато інших.

Невід'ємною частиною безпеки ГПВЧ та ГПВП є аудит цих генераторів. Процес включає систематичний аналіз та перевірку внутрішньої структури і функціонування, виявлення можливих слабкостей, помилок і недоліків, а також оцінку відповідності міжнародним та національним стандартам безпеки. Аудит також спрямований на виявлення потенційних вразливостей і уразливих місць, які можуть бути використані для атак, і на оцінку стійкості генераторів до різних видів атак, включаючи статистичні, аналітичні, криптоаналітичні та інші. Результати надають важливу інформацію для подальшого вдосконалення та розвитку ГПВЧ, спрямованих на підвищення рівня безпеки цих систем. Захистити ГПВЧ від різних атак можна і використовуючи певні заходи [17]. Наприклад, потрібно використовувати хеш-функцію для захисту вразливих вихідних даних ГПВЧ.

Якщо існує підозра, що ГПВЧ є вразливим до прямої криптоаналітичної атаки, тоді виходи з ГПВЧ слід попередньо обробити за допомогою криптографічної хеш-функції. Не всі можливі недоліки ГПВЧ будуть усунуті навіть після хешування їхніх виходів, тому це не гарантує повної безпеки, але підвищує її ймовірність.

Щоб запобігти більшості атак із вибраним введенням, вхідні дані слід хешувати за допомогою позначки часу або лічильника перед надсиланням у PRNG. Якщо це занадто дорого, щоб робити щоразу, коли вхід обробляється, розробник системи може хешувати лише ті вхідні дані, які ймовірно можуть бути під контролем зловмисника.

Час від часу варто генерувати новий початковий стан ГПВЧ, наприклад, для ANSI X9.17, які залишають значну частину свого стану незмінною після ініціалізації. Це гарантує, що будь-який ГПВЧ зможе повністю перезавантажитися за достатнього часу та вхідної ентропії.

Особливу увагу потрібно звертати на вихідні точки ГПВЧ і вихідні файли. Найкращий спосіб захистити ГПВЧ та ГПВП від атак на компроміс стану полягає в тому, щоб стан генератора ніколи не потрапив у руки зловмисника. Важливо розробляти систему так, щоб ініціалізація ГПВЧ відбувалася з непередбачуваної точки і щоб обробка початкових файлів проводилася ретельно.

Базуватись ГПВЧ повинні на чому-небудь сильному, тобто мають бути розроблені так, щоб успішна пряма криптоаналітична атака передбачала успішну атаку на криптографічний примітив, який вважається міцним. Найкраще, це має бути математично доведено.

Для безпеки ГПВЧ та ГПВП важливо, що весь внутрішній стан ГПВЧ змінюється з часом. Це запобігає тому, щоб компроміс одного стану став безповоротнім.

Щоб захистити генератори псевдовипадкових чисел та послідовностей від ймовірних атак, варто проводити " catastrophic reseeding". Частина внутрішнього стану, яка використовується для генерації виходів, повинна бути відокремлена від ентропійного басейну. Стан генерації повинен зміню-

ватися тільки тоді, коли зібрано достатньо ентропії для опору ітеративним атакам на здогад.

ГПВЧ має бути розроблений таким чином, щоб протистояти зворотному відстеженню. В ідеалі це означало б, що на практиці вихід t був неможливим для зловмисника, який скомпрометував стан ГПВЧ у момент часу t + 1. Також може бути прийнятним просто передавати стан ГПВЧ через односторонню функцію кожні кілька виходів, обмежуючи можливий масштаб будь-якої зворотної атаки.

Вхідні дані для ГПВЧ повинні комбінуватися в стані ГПВЧ таким чином, щоб, з використанням невідомої послідовності входів, атакувальник, який спочатку знає стан ГПВЧ, але не знає послідовності входів, і атакувальник, який спочатку знає послідовність входів, але не стан, обидва не могли здогадатися про кінцевий стан. Це забезпечує захист від атак із вибраним введенням і атак розширення на компроміс стану.

Ще один захід безпеки – швидке відновлення після компромісу. ГПВЧ повинен використовувати кожен біт ентропії у вхідних даних, які він отримує. Якщо зловмисник хоче дізнатися вплив послідовності входів на стан ГПВЧ, йому доведеться здогадатися про всю послідовність входів.

Загалом, існує дуже великий спектр заходів безпеки, адже зі зростанням кількості атак на генератори псевдовипадкових чисел, збільшилась потреба і в надійних ГПВЧ. Кожен захід безпеки є кроком у забезпеченні цієї надійності та має велике значення в унеможливленні атак і збереженні конфіденційності даних.

ВИСНОВКИ

Підсумовуючи варто зазначити, що безпека генераторів псевдовипадкових чисел є надзвичайно актуальною та відіграє важливу роль у сучасному цифровому світі. Досягнення високого рівня безпеки ГПВЧ та ГПВП є ключовим завданням, адже через певні вразливості в методах, алгоритмах та способах побудови таких генераторів існує широкий спектр потенційних атак, які можуть серйозно підірвати їхню надійність та навіть призвести до катастрофічних наслідків у різних сферах застосування даних генераторів, особливо в сфері кібербезпеки, криптографії та інформаційної безпеки, таких як розкриття конфіденційної інформації та підрив криптографічних систем. Особливо це стосується використання генераторів у сферах з високими вимогами до їх надійності та захисту.

Із зростанням популярності використання ГПВЧ та ГПВП збільшується ймовірність різноманітних атак на них. У цьому контексті, розуміння суті атак, методів та способів їх реалізації, а також можливих наслідків відіграє важливу роль у розробці надійних стратегій захисту і забезпечення безпеки в інформаційному середовищі. Захист від таких атак стає дедалі важливішим, оскільки від нього залежать конфіденційність та надійність інформації. Спільні зусилля розробників та дослідників таких генераторів повинні бути спрямовані на розробку більш безпечних методів генерації псевдовипадкових чисел і послідовностей.

Знання та впровадження ефективних заходів безпеки є необхідними, оскільки це може суттєво знизити ризики, пов'язані з можливими атаками, стати бар'єром перед небажаними діями зловмисників.

У світлі постійної еволюції кіберзагроз і зростаючого обсягу даних, присвячених генерації псевдовипадкових чисел, класифікація атак та основних причин, які до них призводять, що запропонована в даній роботі, стане корисною для фахівців та інших зацікавлених сторін, оскільки дозволить визначити напрямки подальших досліджень щодо розробки більш ефективних та більш надійних ГПВЧ та ГПВП.

ЛІТЕРАТУРА

[1] Shujun, L., Xuanqin, M., Yuanlong, C. (2001). Pseudo-random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream-Cipher Cryptography. In: Rangan, C.P., Ding, C. (eds) Progress in Cryptology, INDOCRYPT 2001. Lecture Notes in Computer Science, vol 2247. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45311-3_30.

[2] 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.

[3] Хомік М.А., Гарасимчук О.І., Застосування генераторів псевдовипадкових чисел та послідовностей в кібербезпеці, методи їх побудови та оцінки якості. Захист інформації, том 25, № 3, липень-вересень 2023, С 147-159.

[4] Поперешняк С.В. Застосування генератора псевдовипадкових чисел для підвищення ефективності технології smart dust в управлінні розумним будинком. Телекомунікаційні та інформаційні технології. 2022. № 4 (77).

[5] 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.

[6] Melosik, M., Galan, M., Naumowicz, M., Tylczyński, P., & Koziol, S. (2023). Cryptographically Secure PseudoRandom Bit Generator for Wearable Technology. Entropy, 25(7), p. 976.

[7] Maldonado, M. J., & Maldonado, J. L. (2023). A novel hybrid mechanism for generation of pseudo-random sequences for data protection purposes. International Journal of Computers, 17, pp. 1-7.

[8] Hameedi, B. A., Hattab, A. A., & Laftah, M. M. (2022). A Pseudo-Random Number Generator Based on New Hybrid LFSR and LCG Algorithm. Iraqi Journal of Science, pp. 2230-2242.

[9] Ambili, K. N., & Jose, J. (2022). Reinforcing Lightweight Authenticated Encryption Schemes against Statistical Ineffective Fault Attack. Cryptology ePrint Archive.

[10] Zhang, X., Qin, Z., & Zhang, Q. (2023, June). Research on the pseudorandom sequence generator based on compertz map and piecewise map. In International Conference on Cyber Security, Artificial Intelligence, and Digital Economy (CSAIDE 2023) (Vol. 12718, pp. 71-76). SPIE.

[11] AL-khatib, M. A. S., & Lone, A. H. (2018). Acoustic lightweight pseudo random number generator based on cryptographically secure LFSR. International Journal of Computer Network and Information Security, 12(2), p. 38.

[12] Ripley, B. D. (1990). Thoughts on pseudorandom number generators. Journal of Computational and Applied Mathematics, 31(1), pp. 153-163.

[13] Peach, P. (1961). Bias in pseudo-random numbers. Journal of the American Statistical Association, 56 (295), pp. 610-618.

[14] Barker, E. B., & Kelsey, J. M. (2007). Recommendation for random number generation using deterministic random bit generators (revised) (pp. 800-900). Washington, DC, USA: US Department of Commerce, Technology Administration, National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory.

[15] Ruhault, S. (2017). SoK: Security models for pseudo-random number generators. IACR Transactions on Symmetric Cryptology, pp. 506-544.

[16] Almaraz Luengo, E. (2022). A brief and understandable guide to pseudo-random number generators and specific models for security. Statistic Surveys, 16, pp. 137-181.

[17] Kelsey, J., Schneier, B., Wagner, D., & Hall, C. (1998, March). Cryptanalytic attacks on pseudorandom number generators. In International workshop on fast software encryption (pp. 168-188). Berlin, Heidelberg: Springer Berlin Heidelberg.

[18] Sidorenko, A., & Schoenmakers, B. (2005). State recovery attacks on pseudorandom generators. In WEWoRC 2005, Western European Workshop on Research in Cryptology. Gesellschaft für Informatik eV.

[19] Röck, A., 2005. Pseudorandom number generators for cryptographic applications, p. 131.

[20] Zenner, E. (2004). On cryptographic properties of LFSR-based pseudorandom generators.

[21] Мандрона М.М., Гарасимчук О.І. Атаки на генератори псевдовипадкових чисел. // Вісник НУ "Львівська політехніка" – "Автоматика, вимірювання та керування", №741. 2012, С. 251-256.

[22] Desai, A., Hevia, A., & Yin, Y. L. (2002, April). A practice-oriented treatment of pseudorandom number generators. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 368-383). Berlin, Heidelberg: Springer Berlin Heidelberg.

[23] Couteau, G., Dupin, A., Méaux, P., Rossi, M., & Rotella, Y. (2018, October). On the concrete security of Goldreich's pseudorandom generator. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 96-124). Cham: Springer International Publishing.

[24] Johansson, T., & Jönsson, F. (2000). Fast correlation attacks through reconstruction of linear polynomials. In Advances in Cryptology—CRYPTO 2000: 20th Annual International Cryptology Conference Santa Barbara, California, USA, August 20-24, 2000 Proceedings 20 (pp. 300-315). Springer Berlin Heidelberg.

[25] Гулак, Г. М., Мухачов, В. А., Хорошко, В. О., & Яремчук, Ю. Є. (2011). Основи криптографічного захисту інформації: підручник. Вінниця: ВНТУ, С. 72-79.

[26] Johansson, T., & Jönsson, F. (1999). Fast correlation attacks based on turbo code techniques. In Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19 (pp. 181-197). Springer Berlin Heidelberg.

[27] Горбенко, С. І., Шапочка, Н. В., Гріненко, Т. О., Нейванов, А. В., & Мордвінов, Р. І. (2011). Методи та засоби генерування псевдовипадкових послідовностей.

[28] Chose, P., Joux, A., & Mitton, M. (2002). Fast correlation attacks: An algorithmic point of view. In Advances in Cryptology – EUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques Amsterdam, The Netherlands, April 28-May 2, 2002 Proceedings 21 (pp. 209-221). Springer Berlin Heidelberg.
[29] ISO/IEC 18031:2011 Information technology – Security techniques – Random bit generation URL: https://www.iso.org/standard/54945.html.
[30] ISO/IEC 18032:2020 Information security – Prime number generation. URL: https://www.iso.org/standard/72009.html.
[31] ДСТУ ISO/IEC 19790:2015 Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів (ISO/IEC 19790:2012, IDT). URL: http://shop.uas.org.ua/ua/informacijni-tehnologii-metodi-zahistu-vimogi-bezpeki-do-kriptografichnih-moduliv.html.
[32] 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).
[33] Min, Lequan et al. "Analysis of FIPS 140-2 Test and Chaos-Based Pseudorandom Number Generator." (2013).

ANALYSIS OF THREATS TO GENERATORS OF PSEUDO-RANDOM NUMBERS AND PSEUDO-RANDOM SEQUENCES AND PROTECTION MEASURES

In the modern digital world with diverse applications, including cryptography, cybersecurity, and data protection, the issue of building reliable and secure pseudorandom number and sequence generators has become particularly significant. These generators create numerical sequences that appear random but are, in fact, deterministic and possess a certain structure, making them valuable in various fields. They are used for generating secret keys, ensuring confidentiality, data integrity, and transaction security, so their security is critical for applications that employ such generators. However, as the popularity and scope of pseudorandom number generators and pseudorandom sequence generators grow, so does their vulnerability to different types of attacks. Attacks on these generators can lead to the exposure of secret parameters and the compromise of security systems. Malicious actors and hackers seek various vulnerabilities in the methods and algorithms used to construct such generators to partially or fully disclose their operational principles. In this work, based on a thorough analysis of scientific publications by experts involved in the development, research, evaluation of quality, and application of pseudorandom number and sequence generators, the main vulnerabilities of these generators have been identified and described. Different types of attacks have been classified and described, and their impact on these generators has been determined. Security recommendations have been provided, and standards and testing methods have been identified to enhance the reliability, protection, and mitigation of vulnerabilities of such generators.
Keywords: generators of pseudo-random numbers, generators of pseudo-random sequences, cyber security, generation, vulnerabilities, attacks, 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: 10.18372/2410-7840.25.18223
УДК 004.621.5

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЩОДО КІБЕРЗАХИСТУ ДЕРЖАВИ ВІД КІБЕРАТАК

Наталія Блавацька, Микола Браіловський, Валерій Козюра, Володимир Хорошко

Захист об'єктів критичної інфраструктури держави від кібератак, тим більше в умовах бойових дій, вимагає від державних органів вжити ефективних заходів кіберзахисту. В основі таких заходів лежить розробка державних цільових програм кіберзахисту. При формуванні вимог до сучасних систем кіберзахисту