УДК 004.005:004.9
DOI https://doi.org/10.32782/2663-5941/2026.1.2/10

Добровольський Ю.Г.
https://orcid.org/0000-0002-1248-3615
Чернівецький національний університет імені Юрія Федьковича

Дячук Р.Л.
https://orcid.org/0000-0002-6259-3302
Чернівецький національний університет імені Юрія Федьковича

ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ГЕНЕРАЦІЇ ПОСЛІДОВНОСТІ ВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ ВИМІРЯНИХ ЗНАЧЕНЬ ТЕМНОВОГО СТРУМУ ФОТОДІОДУ

Безпека інформаційних потоків є визначальним фактором сучасного цифрового світу. Вона забезпечується за допомогою інформаційних технологій, які об'єднують у собі кілька напрямів та спеціальностей. Послідовності випадкових чисел є одним елементів захисту інформаційних потоків, які дозволяють убезпечувати їх при формуванні, обробці, передачі та декодуванні. Корисна інформація за звичай, розчиняється у послідовності випадкових чисел за певним правилом. Існує багато методів формування таких числових послідовностей. Усі вони базуються на джерелі хаотичних, безсистемних сигналів. Ступінь хаотичності таких сигналів визначає, зокрема, ступінь надійності згенерованої за їх допомогою, хаотичних послідовностей. Тому розробка надійних методів генерації непередбачувані послідовності випадкових чисел є надзвичайно актуальним завданням програмної інженерії.

Однак, методи генерації послідовностей випадкових чисел мають бути доступні для застосування в адоптованому стані. А саме – у вигляді інформаційної системи, яка має зрозумілий та зручний інтерфейс та внутрішню логіку. В нашому випадку застосовується метод генерації послідовності випадкових чисел на основі виміряних значень темнового струму фотодіода, які є абсолютно не передбачуваними.

З огляду на вище наведене, метою роботи є розробка інформаційної системи для генерації послідовності випадкових чисел на основі темнового струму фотодіоду.

В ході дослідження було створено апаратну частину інформаційної системи. Розроблено установку для вимірювання темнового струму фотодіоду при 50 °С із забезпеченням певної кількості вимірювань в одиницю часу і передачі виміряних значень темнового струму до комп'ютера за допомогою USB адаптера. Створена інформаційна система генерує послідовності випадкових чисел, перевіряє її на відповідність критеріях хаотичності, в основу якого покладено середньоквадратичне відхилення отриманих числових значень, яке має бути не більше 0,39. Накопичує перевірені послідовності випадкових чисел у відповідну бібліотеку.

В основу архітектури інформаційної системи покладено ієрархію інформаційної безпеки з одного боку і принципи CIA з другого. Розроблений інтерфейс генерації, дослідження та використання послідовностей випадкових чисел, в основу якого покладено можливість обрання балансу між швидкість генерації послідовності випадкових чисел та її надійністю.

Ключові слова: *інженерія програмного забезпечення, інформаційна система, кібербезпека, фотодіод, темновий струм, випадкові числа, надійність програмного забезпечення.*

Постановка проблеми. Цифровізація суспільства надає багато переваг у його розвитку, але і створює суттєві загрози. Дані користувачів цифрових систем, які зберігаються у різноманітних цифрових сховищах, мають надійно зберігатися, а доступ до них має бути суворо структурованим згідно пріоритетів, встановлених законодавчою базою. А саме – цифрові потоки даних мають бути захищені, в тому числі методами програмної інженерії, зокрема криптографії. Актуальність цього питання зумовлена не тільки здоровим глуздом, а рішеннями уряду України. Закон України

№ 3534-IX, про зміни до законів України, зокрема «Про пріоритетні напрями розвитку науки і техніки» та «Про пріоритетні напрями інноваційної діяльності в Україні» від 13.01.2024 року, відносять до пріоритетних напрямків розвитку держави інформаційні та комунікаційні технології.

Інформаційні технології об'єднують у собі кілька напрямів та спеціальностей, фахівці яких здатні вирішувати питання забезпечення безпеки даних, що зберігаються, або передаються, від несанкціонованого доступу. Одним з напрямків захисту інформаційних потоків даних є створення програмного забезпечення на основі послідовності випадкових чисел (ПВЧ), які додаються до основного інформаційного пакету. В цьому випадку корисна інформація розчиняється у ПВЧ, або знаків за певним правилом, відомим як відправнику так і отримувачу інформації.

Отже, джерело хаотичних сигналів, або хаосу, може бути базою для генерації непередбачуваних числових послідовностей, або випадкових послідовностей. Їх можна використовувати, як зазначалось вище, для безпечних, надійних та ефективних з'єднань, створення криптографічних ключів, дослідження цілісності систем та інших напрямках [1].

Таким чином, розробка надійних методів генерації непередбачувані ПВЧ є надзвичайно актуальним завданням програмної інженерії.

Аналіз останніх досліджень і публікацій. Розрізняють псевдо-хаотичні послідовності і власне, хаотичні послідовності.

До псевдо-хаотичних послідовностей відносять послідовності, отримані програмними методами, які досить легко передбачити [2]. Окрім того, вони досить легко доступні, оскільки, більшість з них є у відкритому доступі. Прикладом може слугувати генерації псевдовипадкових числових послідовностей, отримані на мові Java [3]. Вони, теоретично, можуть бути доступні для використання у атаках на шифрувальні послідовності. Загроза успішності подібних дій пов'язана із розвитком обчислювальної техніки, зокрема, її апаратної частини, застосування квантових обчислень у цьому питанні [4, 5], збільшує успішність зламу до рівня практичного застосування.

Для створення хаотичних послідовностей залучають також певні подій, які відбуваються у цифровій техніці. Такий підхід здатний забезпечити генерацію числової послідовності, близької за своїми властивостями, до хаотичної послідовності. Прикладом може слугувати лічильник тактової частоти процесора у комп'ютері. Його недолік – залежність від зовнішнього впливу, який може втрутитися у генерацію випадкових числових послідовностей [6]. Також джерелом випадкової ПВЧ може бути оптичний маніпулятор миші [7]. Послідовності, отримані таким методом, можуть мати досить неоднорідний розподіл. Але, він є повільним, оскільки його швидкість генерації не перевищує 1 кбіт/с. Отже, він не може бути застосований для швидкодіючих шифрувальних систем.

Нещодавно запропоновано здійснювати генерацію випадкової ПВЧ за допомогою веб-камери [8, 9]. Показано, що зміна інтенсивності пікселів веб-камери, в кожен момент часу, має непередбачуваний характер.

Спираючись на результати, наведені у [8, 9] нами було запропоновано і досліджено генерацію ПВЧ, отриману на основі темнового струму фотодіоду на основі кремнію, який працює у фотодіодному режимі. Виявилося, що фотодіод, а саме його темновий струм, може слугувати джерелом для генерації випадкових чисел. Такий набір чисел є рівномірно-хаотичним. При цьому кожне число у послідовності зустрічається рівномірно у діапазоні 0.3 – 0.7 %. Також виявилося, що темновий струм фотодіоду, виміряний про температурі 50 °С дозволяє згенерувати ще кращу ПВЧ. При цьому кожне число у ПВЧ представлене рівномірно, не частіше 0.18 %, що дозволяє стверджувати про те, що характеристика розподілу по значенню випадкових чисел зсувається у бік «рівномірно-хаотичного».

У подальшому постало завдання створити інформаційну систему для генерації ПВЧ на основі темнового струму фотодіоду.

Постановка завдання. Метою статті є розробка інформаційної системи для генерації ПВЧ на основі темнового струму фотодіоду. Для досягнення мети роботи потрібно було розв'язати наступні завдання.

1. Створення апаратної частини інформаційної системи. А саме.

1.1. Забезпечення вимірювання темнового струму фотодіоду при 50 °С із забезпеченням певної кількості вимірювань в одиницю часу.

1.2. Забезпечення передачі виміряних значень темнового струму до комп'ютера.

2. Створення ПВЧ.

3. Забезпечення перевірки ПВЧ на відповідність критеріях хаотичності.

4. Формування інформаційної системи для генерації ПВЧ на основі вимірювання темнового струму фотодіоду.

Виклад основного матеріалу. Створення апаратної частини інформаційної системи. Для вирішення поставлених завдань було розроблено установку для генерації ПВЧ на основі виміряних значень темнового струму кремнієвого фотодіода ФД-288 [10]. Блок-схема установки наведена на рисунку 1.

Установка працює наступним чином. Фотодіод ФД-288 (3) закритий світлонепроникним екраном (2) і разом з ним розміщений у термостаті типу НВ120-S [11] (1), який має діапазон підтримування температур від 5 до 120 °С з точністю 0,5 °С і живиться як від мережі, так і від блоку живлення (5). На термостаті встановлюється температура 50 °С. За допомогою блоку живлення фотодіоду (4) на ньому встановлюється зміщення 10 мВ. Виміряне значення темнового струму фотодіоду перетворюється у напругу за допомогою прецизійного перетворювача струм-напруга (ППСН) (7), підсилюється підсилювачем (8) для подальшої обробки аналогово-цифровим перетворювачем (9) з метою отримання цифрового сигналу, еквівалентного темновому струму, який оброблюється процесором Arduino (112593) (10) для адаптування цифрового сигналу і передачі його до USB-адаптера (11), за допомогою якого цифровий сигнал передається до USB порту комп'ютера (12), з якого потрапляє до процесора комп'ютера (13).

Керування встановленням напруги на фотодіоді, температури фотодіода, тривалістю відбору значень темнових струмів, кількості вимірів в одиницю часу, здійснюється за допомогою інтерфейсу інформаційної системи.

Підсилення сигналу темнового струму на 5 Вольт, переводить характеристику розподілу по значенню псевдовипадкових чисел у бік «рівномірно-хаотичної».

Створення ПВЧ

Формування ПВЧ здійснюється згідно алгоритму, наведеному на рисунку 2.

Виміряні значення напруги, яка еквівалентна темновому струму фотодіода, у вигляді вхідного потоку даних опрацьовуються комп'ютером із використанням мови програмування Java (17 версія). При цьому застосовується бібліотеки javax-usb, за допомогою якої вхідні дані завантажуються у певний список. При цьому вони вважаються випадковими числами від 0 до 10. Далі отриманий список чисел вивчається на відповідність статистичним вимогам із використанням бібліотеки Descriptive Statistics. Бібліотеки jfree.chart та jfree.data застосовуються для графічного представлення статистичних характеристик ПВЧ.

Забезпечення перевірки ПВЧ на відповідність критеріях хаотичності

Як відомо [12] ідеальний рівномірний розподіл повинен мати середньо квадратичне відхилення (Z_{mean}) на рівні 0,39. Тому основним критерієм ідеально рівномірного розподілу в нашому випадку обрано саме цю величину – середньоквадратичне відхилення. Програмно згенерована послідовність має відхилення від середнього не більше 0,002 [13]. Як що отримана ПВЧ відповідає цьому критерію, вона направляється до бібліотеки ПВЧ. Як що не відповідає – відкидається, або формується повторно.

Окрім того, має відбуватися перевірка на відповідність іншим критеріям, таким як мінімальне (Z_{min}) і максимальне значення (Z_{max}) співпадінь однакових чисел у послідовності. Ці значення мають бути також в осередку 0,39. Також варто

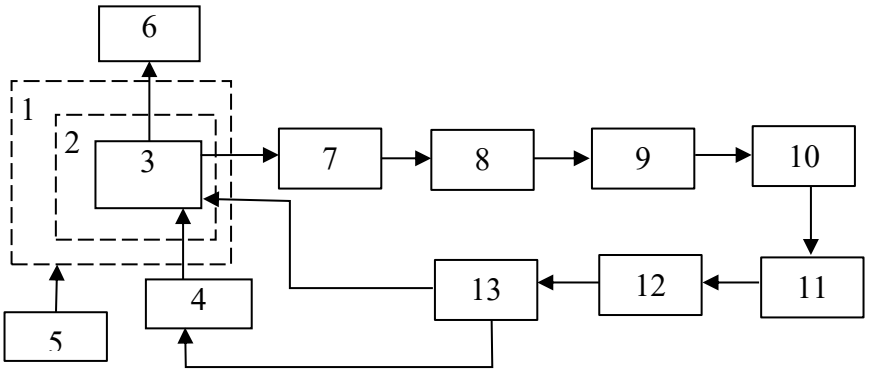

Рис. 1. Блок-схема установки для генерації ПВЧ на основі виміряних значень темнового струму кремнієвого фотодіода ФД-288: 1 – термостат; 2 – світлонепроникний екран, 3 – фотодіод, 4 – блок живлення фотодіода, 5 – блок живлення термостата, 6 – термометр цифровий Тензор-42, 7 – ППСН, 8 – підсилювач постійної напруги; 9 – аналогово-цифровий перетворювач; 10 – центральний процесор Arduino (112593), 11 – USB-адаптер, 12 – USB порт комп'ютера, 13 – процесор комп'ютера

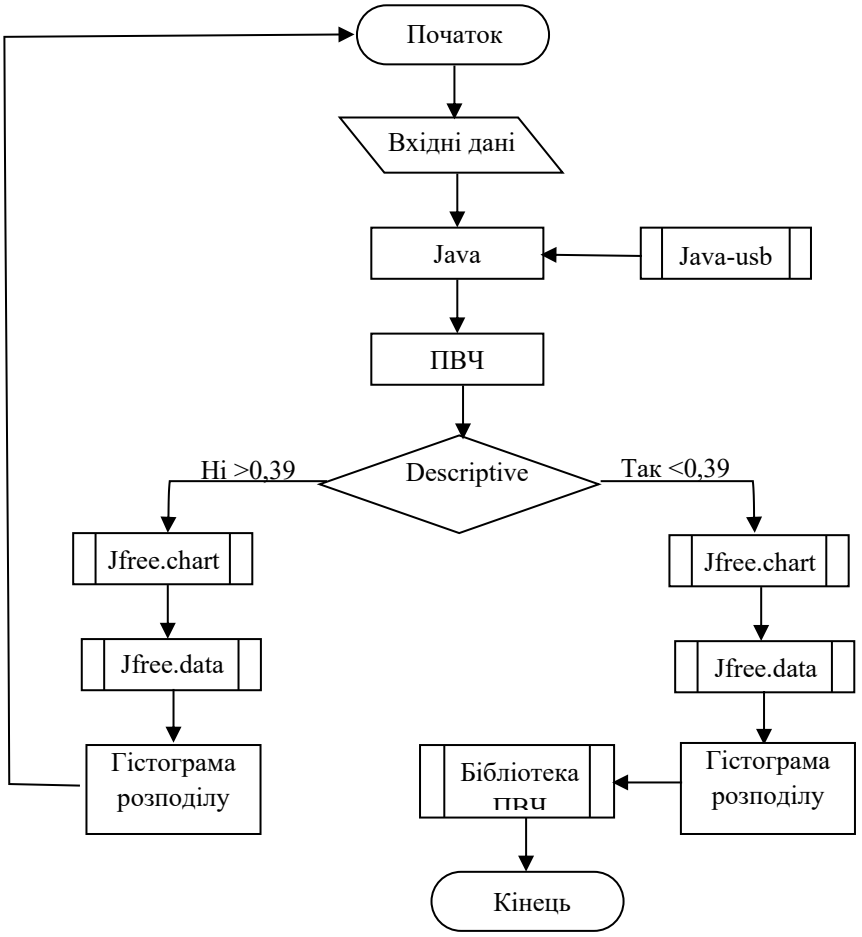

Рис. 2. Алгоритм формування ПВЧ

враховувати процент відсутніх елементів (Z_{absent}), який має складати 0 %.

Зрозуміло, що оскільки вимоги до Z_{mean}, Z_{min}, та Z_{max} є однакові – не повинні перевищувати 0,39, то можна обмежитись вимірюванням значення Z_{mean}.

Але, для забезпечення точності вимірів варті ці показники контролювати. Тому у рамках інформаційної системи, коли на формування ПВЧ не впливає час, ці параметри мають перевірятись.

Формування інформаційної системи для генерації ПВЧ на основі вимірювання темнового струму фотодіоду.

Основне завдання створюваної інформаційної системи полягає у генерації ПВЧ з одного боку, захищеності системи від стороннього втручання з другого та зручність користування користувачем з третього.

Сформуємо основні вимоги до такої інформаційної системи.

1. Має бути реалізований принципи CIA (confidentiality, integrity, availability, або конфіденційність, цілісність, доступність).

2. Має бути створена ієрархія інформаційної безпеки, яка має містити управління згенерованими ХЧП, інформаційний та мережевий менеджмент, системний, сервісний і бізнес-рівень, а також постійний моніторинг вимог бізнес-процесу. Також інформаційна система має відслідковувати таки чинники як політичні та законодавчі зміни. Ці фактори повинні мати безперервний аудит.

3. Має бути зручний інтерфейс генерації, дослідження та використання ПВЧ.

Реалізація принципів CIA.

Кожна з перерахованих вище завдань реалізується у вигляді мікросервіса в загальному контексті архітектури "N-tyer", тобто багаторівневої архітектури.

В основі роботи розробленої інформаційної системи лежить принцип ієрархічності допусків власника, менеджерів та користувачів системи, як це показано на рисунку 3.

CIA повинна мати документальну базу, а також затверджену регуляторну політику. В них документально мають бути визначені вимоги до параметрів і показників, за якими потрібно

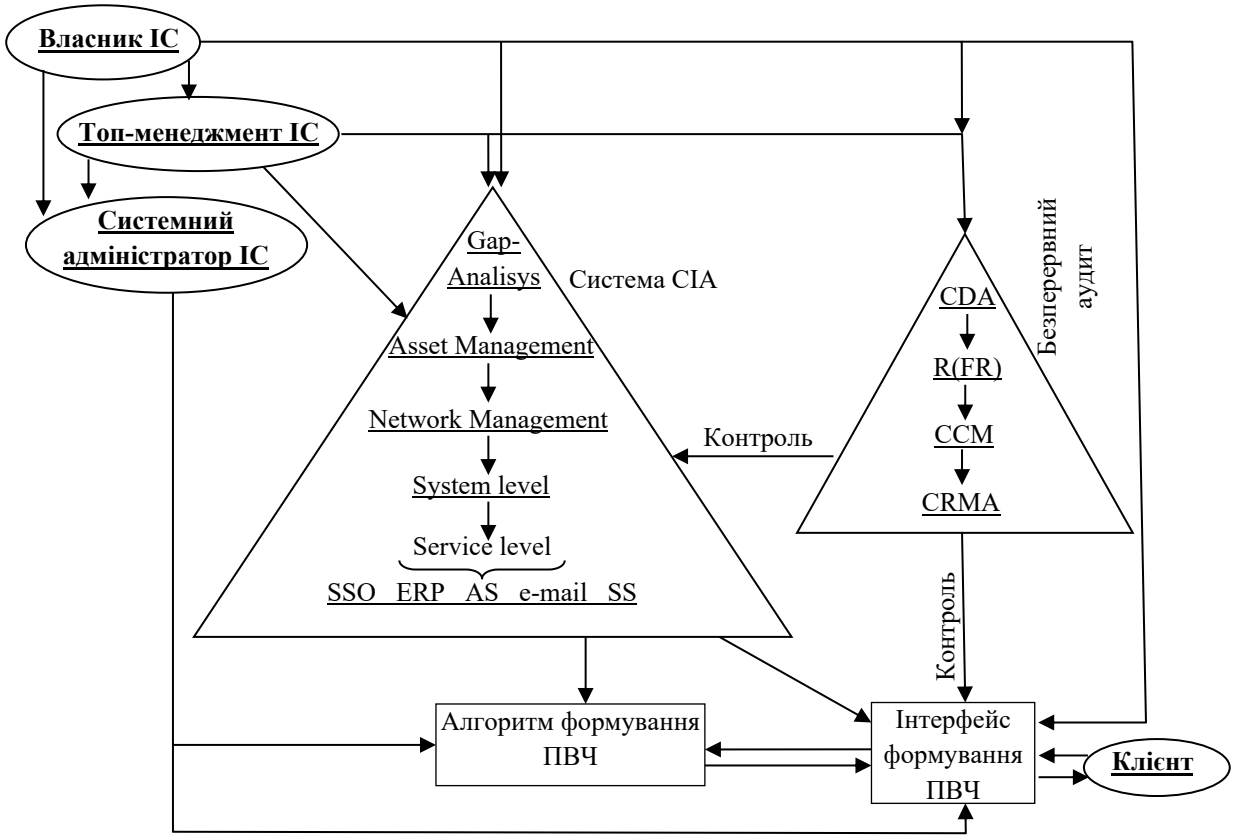

Рис. 3. Архітектура інформаційної системи

безперервно стежити (монітори). Це дозволить своєчасно реагувати системі на загрози. Регуляторна політика має формуватися на основі принципу Gap-Analisys. А саме – оцінці зазорів (gap) між ймовірним зламом і арсеналом протидії зламу.

Основні вимоги гарантії безпеки CIA.

C – confidentiality – забезпечення недоступності до закритої (конфіденційної) інформації для не уповноваженої особи або процесу (бота, сканування, тощо).

I – integrity – властивість підтримки правильності і повноти активів. Якщо з'являється нова загроза (ризик), то наш арсенал повинен мати можливість, бути доповнене. Оцінка ризику також завдання не просте.

A – availability – властивість бути доступним і готовим до використання за запитом уповноваженої особи.

Ієрархія інформаційної безпеки передбачає управління активами (Asset management). Будь-який матеріальний носій або передавач інформації є Ассет. Жорсткі, диски, роутери, комп'ютери, мобільні телефони, флешпамяті, CD-ROM. Всі ці Ассет можуть бути використані для несанкціонованого доступу або витоку інформації.

Інформаційний менеджмент Ассет – набір всіх даних, правил і процедур, які в сукупності представляють собою концепцію, значиму для бізнесу. Будь-який збій в цьому алгоритмі повинен знайти відгук в системі безпеки.

Network Management (Мережевий менеджмент) передбачає моніторинг ризиків пов'язаних з несанкціонованого доступу до інформації при передачі через мережі.

System level (Системний рівень) передбачає моніторинг системного рівня і відстеження подій/змін в роботі: domain контролерів; бази даних; сховища даних; серверних додатків; систем віртуалізації; операційних систем; хмарних кластерів.

Service level (Сервісний рівень) розділяється на SSO – Single Sign-On (Система єдиного входу), ERP (enterprise resource planning – планування ресурсів підприємства), AS (authorization service – сервіс авторизації), e-mail сервіс, SS (supporting services – допоміжні сервіси).

Складовою частиною безперервного аудиту (моніторингу) є:

CDA – безперервне забезпечення цілісності даних (Continuous data assurance). CDA перевіряє цілісність даних, що проходять через інформаційні системи.

Основними методами забезпечення цілісності інформації (даних) при зберіганні в автоматизованих системах є:

– R(FR) (Reliability (failure resistance) – надійність (відмово стійкість) – надмірність, дублювання, віддзеркалення обладнання та даних, наприклад, за рахунок використання RAID-масивів;

– безпечне відновлення (резервне копіювання і електронне архівування інформації).

CCM (Continuous control monitoring) – безперервний моніторинг управління ресурсами. CCM забезпечує постійний моніторинг використання ресурсів, порівнюючи їх із заздалегідь визначеними ключовими показниками для виявлення нештатних ситуацій. Найбільш поширеним рішенням CCM є створення Центру управління безпекою (SOC). CCM також включає регулярне сканування компонентів IT-інфраструктури на наявність вразливостей. Часто ці обов'язки покладаються на системного адміністратора і технічної підтримки.

CRMA (Continuous risk monitoring and assessment) – постійний ризик-моніторинг. В рамках CRMA аналізуються результати CCM і CDA, а також аналізуються і прогнозуються ризики і можливі втрати. В рамках CRMA відбувається управління ризиками – процес прийняття і реалізації управлінських рішень, спрямованих на зниження ймовірності інцидентів і мінімізацію втрат. Найбільш часто використовуваним інструментом управління ризиками є страхування.

Інтерфейс формування ПВЧ.

Інтерфейс формування ПВЧ побудований на основі співвідношення між балансом (швидкодією) і безпечністю (надійністю), наведений на рисунку 4.

Наступні параметрі в налаштуваннях інтерфейсу інформаційної системи впливають на це співвідношення. А саме:

– можна обрати кількість вимірювань. Це актуально лише для realtime вимірювання.

– можна вказати на якій кількості вимірювань потрібно генерувати ПВЧ.

Очевидно, що кількість кіл якихось обробок тих вимірювань для створення ПВЧ, сповільнює саму генерацію, але робить ПВЧ більш надійною. Тому у інтерфейсі передбачена можливість налаштування часу вимірювання і часу генерації ХЧП.

Секція Value Range Configuration дозволяє обрати які значення будемо генерувати.

Секція Data Source Settings дає можливість вибрати джерело звідки потрібно брати значення вимірювання.

Вимірювання RealTime і налаштування для нього. Тут може бути обрано вимірювання з файлу. Може знадобитись для відтворення (як Seed).

На вкладці з генерацією ПВЧ можна вказати розмір ПВЧ і згенерувати її. Результат буде відображено в Generated Sequence. Також у а також Generated Sequence можнка отримати короткий аналіз отриманої ПВЧ.

Вкладка 3. Аналіз отритманої ПВЧ.

Одразу при переході на неї виконується тестування, конкретної ХЧП на випадковість Randomness Test і демонструються результати тестування. Chaotic Properties показує характеристики хаотичності. Також передбачена секція, яка дає візуалізацію розподілення по значенням. В якості прикладу на рисунку 6 наведено візуалізацію розподілення по значенням однієї зі згенерованих ПВЧ.

Інтерфейс передбачає можливість порівнювати попередні результати.

Остання вкладка показує базу наших згенерованих ПВЧ, а також зберігає їх налаштування, для порівняння і дозволяє завантажувати їх для користувача.

Подальші дослідження передбачають тестування створеної інформаційної системи за функ-

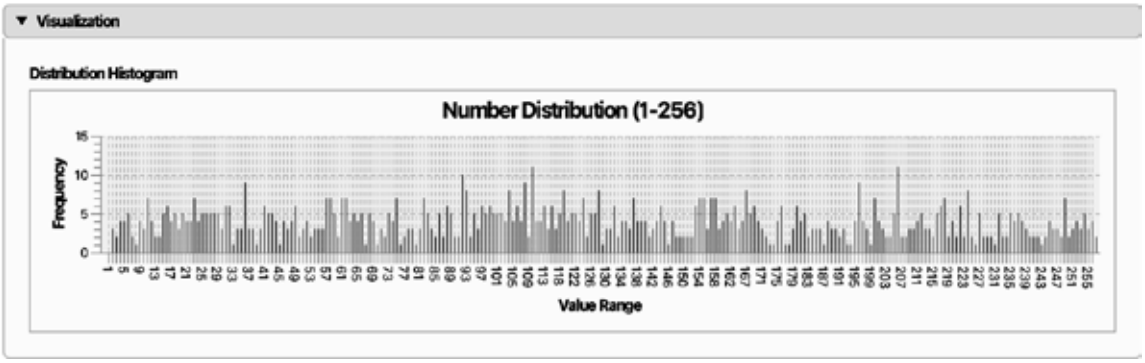

Рис. 5. Приклад візуалізації розподілення по значенням однієї з згенерованих ПВЧ

ціональними вимогами та вивчення ступені її надійності.

Висновки. Розроблено інформаційну систему для генерації ПВЧ на основі темнового струму фотодіоду. Створено апаратну частину інформаційної системи, яка забезпечує вимірювання темнового струму фотодіоду при 50 °С із забезпеченням певної кількості вимірювань в одиницю часу. Забезпечено передачу виміряних значень темнового струму до комп'ютера за допомогою USB адаптера.

Розроблений алгоритм створення ПВЧ. Забезпечено перевірку ПВЧ на відповідність критеріях хаотичності в основу якого покладено середньоквадратичне відхилення отриманих числових значень, яке має бути не більше 0,39.

Сформована інформаційна системи для генерації ПВЧ на основі вимірювання темнового струму фотодіоду. В основу її архітектури покладено ієрархію інформаційної безпеки з одного боку і принципи CIA з другого.

Розроблений інтерфейс генерації, дослідження та використання ПВЧ, в основу якого покладено можливість обрання балансу між швидкість генерації ПВЧ та її надійністю.

Список літератури:

1. Asia O. A. Random Number Generators Survey. International Journal of Computer Science and Information Security (IJCSIS). 2020. Vol. 18, No. 10. https://doi.org/10.5281/zenodo.4249406. (дата звернення: 23.01.2026).

2. Martinez F. Attacks on Pseudo Random Number Generators Hiding a Linear Structure. Cryptographers' Track at the RSA Conference 2022. Mar 2022. Virtual Event. United States. pp. 145–168. URL: https://hal.science/hal-03737675 (дата звернення: 23.01.2026).

3. Class SecureRandom. All Implemented Interfaces. URL: https://docs.oracle.com/javase/8/docs/api/java/security/SecureRandom.html (дата звернення: 23.01.2026).

4. Остапов С.Е., Добровольський Ю.Г. Квантова інформатика та квантові обчислення: навч. посібник. Чернівці : ЧНУ ім. Ю. Федьковича, 2021. – 99 с.

5. Jacak J.E., Jacak W.A., Donderowicz W.A. Wojciech A. Jacak L. Quantum random number generators with entanglement for public randomness testing. *Scientific Reports*. 2020. Vol. 10, № 164. P. 121–130. https://doi.org/10.1038/s41598-019-56706-2

6. Бараннік В. В., Бараннік Н. В., Ігнатьєв О. О., Хіменко А. М. Метод непрямого приховування інформації в процесі стиснення відеозображень. *Радіоелектронні і комп'ютерні системи*. 2021. № 4. С. 119–131. https://doi.org/10.32620/reks.2021.4.10

7. Ostapov S., Diakonenko B., Fylypiuk M., Hazdiuk K., Shumyliak L., Tarnovetska O. Symmetrical Cryptosystems based on Cellular Automata. *International Journal of Computing.* 2023. № 22. P. 15–20. https://doi.org/10.47839/ijc.22.1.2874

8. Diachuk R., Dobrovolsky Y., Hanzhelo D., Prokhorov H., Trembach D. Research the Level of Chaotic and Reliability in Webcam-generated Random Number Sequences. *Security of Infocommunication Systems and Internet of Things.* 2024. Vol. 2, № 1. P. 1–6. https://doi.org/10.31861/sisiot2024.1.01004

9. Dobrovolsky Y., Prokhorov G. Primary processing of an optical image on autonomous mobile optical systems using cellular automata. Proceedings of SPIE 12938. Sixteenth International Conference on Correlation Optics, 129380K (5 January 2024). https://doi.org/10.1117/12.3009624.

10. ФД-288. Технічні характеристики. URL: https://zapadpribor.com/fd-288 (дата звернення: 23.01.2026).

11. Термостаті типу НВ120-S. Технічні характеристики. URL: https://spectrolab.com.ua/ua/p664984190-termostat-dlya-probirok.html (дата звернення: 23.01.2026).

12. Веригіна І. В., Островська О. В. Теорія ймовірностей та математична статистика: Частина 2. Випадкові величини: Лекції і практикум. Київ, КПІ ім. Ігоря Сікорського, 2021. 77 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/4c25bed3-0ae6-4677-b2d2-aa3d047c2910/content (дата звернення: 23.01.2026).

13. Prokhorov H., Trembach D. Research Into the Efficiency of Processing a Numerical Random Sequence by Chaotic-type Cellular Automata. *Security of Infocommunication Systems and Internet of Things.* 2024. Vol. 2, №. 2. P. 02010. https://doi.org/10.31861/sisiot2024.2.02010

Dobrovolsky Yu.G., Diachuk R.L. INFORMATION SYSTEM FOR GENERATION OF RANDOM NUMBERS SEQUENCES BASED ON MEASURED VALUES OF THE DARK CURRENT OF A PHOTODIODE

The security of information flows is a determining factor of the modern digital world. It is ensured by means of information technologies, which combine several areas and specialties. Random number sequences (RNS) are one of the elements of information security, which allow to protect them during formation, processing, transmission and decoding. Useful information, as a rule, dissolves into random numerical sequences according to a certain rule. There are many methods for forming such numerical sequences. All of them are based on the source of chaotic, unsystematic signals. The degree of chaos of such signals determines, in particular, the

degree of reliability of the chaotic sequences generated with their help. Therefore, the development of reliable methods for generating unpredictable random number sequences is an extremely urgent task of software engineering.

However, the methods for generating random number sequences must be available for use in an adapted state. Namely, in the form of an information system that has a clear and convenient interface and internal logic. In our case, the method of generating RNS based on the measured values of the dark current of the photodiode, which are completely unpredictable, is used.

Given the above, the purpose of the work is to develop an information system for generating RNS based on the dark current of the photodiode.

During the investigation, the hardware part of the information system was created. A device was developed for measuring the dark current of a photodiode at 50 °C with the provision of a certain number of measurements per unit of time and the transfer of measured dark current values to a computer using a USB adapter. The created information system generates RNS, checks them for compliance with the chaoticity criteria, which is based on the root mean square deviation of the obtained numerical values, which should be no more than 0.39. Accumulates the checked RNS in the appropriate storage.

The architecture of the information system is based on the hierarchy of information security on the one hand and the principles of CIA on the other. An interface for generation, research and use of RNS has been developed, based on the ability to choose a balance between the speed of RNS generation and its reliability.

Keywords: *Software engineering, information system, cybersecurity, photodiode, dark current, random numbers, software reliability.*

Дата першого надходження статті до видання: 26.01.2026
Дата прийняття статті до друку після рецензування: 27.02.2026
Дата публікації (оприлюднення) статті: 08.04.2026