УДК 519.713

І.Д. ГОРБЕНКО, Н.В. ШАПОЧКА, О.О. КОЗУЛІН

Харківський національний університет радіоелектроніки, Україна

ОБҐРУНТУВАННЯ ВИМОГ ДО ГЕНЕРАТОРІВ ВИПАДКОВИХ БІТІВ ЗГІДНО ISO/IEC 18031

У відповідності до існуючої нормативно-правової бази обґрунтовані та визначені вимоги до генераторів псевдовипадкових послідовностей. Визначено, що в найбільш повній мірі вказаним вимогам відповідає стандарт ISO/IEC 18031 «Інформаційні технології – Методи захисту – Генерація випадкових бітів». Пропонується методика та наводиться результат дослідження основних функціональних моделей генераторів випадкових та псевдовипадкових бітів, що підтверджують перспективність, можливість і умови застосування стандарту ISO/IEC 18031 в Україні.

Ключові слова: *генератор випадкових бітів, випадковість, ентропія, статистичні властивості, методика статистичного тестування.*

Введення

Генерування псевдовипадкових бітів є однією з актуальних та важливих задач криптографії. Вихідні дані генераторів випадкових та псевдовипадкових бітів використовуються у багатьох криптографічних додатках, наприклад, при генеруванні ключів, загальносистемних параметрів та ін. Згідно вимог криптографічних застосунків ці генератори повинні задовольняти ряду складних та суперечливих вимог.

На регіональному та міжнародному рівнях, зважаючи на актуальність вказаних задач, розроблені та широко застосовуються стандарти, що визначають вимоги взагалі до засобів КЗІ, а також до засобів генерування ключів. Проте проблемним і важливим завданням є розробка вимог до генераторів випадкових та псевдовипадкових послідовностей.

При формуванні випадкових та псевдовипадкових послідовностей необхідно надавати гарантію, що їх властивості відповідають певним вимогам. Вказані задачі розв'язуються на основі застосування спеціальних методів та методик тестування. На наш погляд, кращі з таких методик уже закріплені в таких нормативних документах, як: NIST SP 800-22, AIS 31 та FIPS 140-1. На жаль в Україні на сьогоднішній час відсутні національні стандарти, які визначають вимоги та методи перевіряння властивостей вказаних генераторів.

Зараз отримав визнання та застосування міжнародний стандарт ISO/IEC 18031 «Інформаційні технології – Методи захисту – Генерація випадкових бітів», який містить вимоги щодо генерування випадкових послідовностей. На наш погляд, гармонізація цього міжнародного стандарту дозволить в значній мірі усунути бар'єри у міжнародному обміні товарів та послуг у сфері криптографічного захисту інформації (КЗІ), підвищить ступінь відповідності засобів та послуг КЗІ їх функціональному призначенню, забезпечити переносимість, сумісність та масштабуємість комплексів КЗІ, а також забезпечити такий технологічний та технічний рівень систем та засобів КЗІ, що відповідав би сучасному рівню розвитку науки, техніки та технологій у сфері КЗІ.

Стандарт ISO/IEC 18031 встановлює концептуальні моделі, термінологію і вимоги, що відносяться до конструктивних елементів і властивостей систем, які використовуються для генерації випадкових бітів в криптографічних застосуваннях. Цей стандарт, в залежності від вибору джерела ентропії – змінного або фіксованого, визначає два типи генераторів: недетерміновані і детерміновані генератори випадкових бітів.

Згідно ISO/IEC 18031 недетермінований генератор випадкових бітів – це механізм генерації випадкових бітів, який використовує джерело ентропії для генерації випадкового потоку бітів [1].

Детермінований генератор випадкових бітів – це механізм генерації бітів, який використовує детерміновані механізми, такі як криптографічні алгоритми, на джерелі ентропії для генерації випадкового потоку бітів. Цей тип генерації бітів використовує особливі вхідні дані і, якщо необхідно, деякі необов'язкові вхідні дані, які, залежно від їх застосування, можуть бути загальнодоступними [1].

Метою цієї статті є аналіз та обґрунтування можливостей і умов гармонізації та застосування ISO/IEC 18031 в Україні.

1. Вимоги до генераторів випадкових бітів

Важливою перевагою даного стандарту є те, що він визначає цілі і вимоги до генераторів випадкових бітів (ГВБ), які є фундаментальними для захисту криптографічних механізмів, яким необхідні випадкові вхідні дані. Дані цілі і вимоги розглядають ГВБ як чорну скриньку, а тому можуть застосовуватися до будь-якого генератора випадкових бітів, як детермінованого, так і недетермінованого. В основному вимоги є варіаціями формулювання необхідності достатньої випадковості вихідного потоку бітів.

До вихідних даних ГВБ стандарт ISO/IEC 18031 висуває такі цілі і вимоги вищого рівня [1]:

1. Неможливість відрізнити вихідні дані ГВБ від істинних однорідно розповсюджених випадкових бітів. Тобто всі можливі вихідні дані повинні виникати з рівною імовірністю, а серії вихідних даних повинні мати однорідний розподіл.

2. Повинно бути невідомим, яким чином для послідовності вихідних бітів здійснити обчислення будь-якого вихідного, минулого або майбутнього біта.

3. Вихідний потік не повинен повторюватися протягом життєвого циклу ГВБ.

4. З точки зору отримання інформації зловмисником вихідні дані ГВБ не повинні створювати витік секретної інформації, як, наприклад, внутрішній стан.

До роботи ГВБ стандарт ISO/IEC 18031 висуває такі цілі і вимоги вищого рівня [1]:

1. ГВБ не повинен застосовуватись для генерування бітів, якщо він не володіє достатньою ентропією.

2. При виявленні помилки ГВБ повинен або вводити постійний помилковий стан, або мати здатність оновлюватися у випадку втрати або компрометації ентропії, якщо постійний помилковий стан вважається неприйнятним для вимог застосування.

3. Структура і реалізація ГВБ повинні мати визначену межу захисту, наприклад межу ISO/IEC 19790 криптографічного модуля.

4. Вихідні дані ГВБ не повинні давати витік секретної інформації (наприклад, внутрішнього стану).

5. Імовірність «невірного функціонування» ГВБ, при якому порушуються вимоги до вихідних даних (наприклад, поява однакових вихідних даних або малий період повторювання, тобто спостерігається повторювання одних і тих же вихідних даних) повинна бути достатньо малою. Тобто імовірність помилки необхідно узгоджувати із загальною впевненістю у коректності операцій ГВБ, і вона не обов'язково повинна мати таку ж стійкість, як стійкість криптографічного захисту.

6. Структура ГВБ повинна включати методи для заборони передбаченого впливу, маніпулювання або прогнозування вихідних даних ГВБ через спостереження фізичних характеристик генератора (наприклад, енергоспоживання, вимірювання часу або випромінювань).

Згідно стандарту ISO/IEC 18031 необов'язковими можливими вимогами до роботи ГВБ є такі [1].

1. Якщо ГВБ здатний діяти в більш ніж одному режимі, то згідно запиту він має повертати інформацію про режим, в якому він діє.

2. Споживче застосування може вимагати, щоб ГВБ працював у режимі тестування, наприклад, при використанні несекретного початкового значення.

3. ГВБ, що розглядається як прозора скринька, повинен мати зворотну секретність.

4. ГВБ, що розглядається як прозора скринька, може мати пряму секретність. Якщо ця вимога підтримується, то це означає, що при отриманні всієї доступної інформації про ГВБ повинно бути неможливим обчислення або передбачення будь-якого майбутнього біту виходу під час запиту прямої секретності.

До всіх генераторів випадкових бітів стандарт ISO/IEC 18031 висуває такі функціональні вимоги [1].

1. Реалізація ГВБ має проектуватися так, щоб вона могла забезпечувати можливість перевірки достовірності, зокрема, має бути визначено, що не повинен робити ГВБ. Перевірка достовірності недетермінованих ГВБ означає, що поведінка недетермінованих ГВБ є очікуваною не тільки протягом звичайної операції, але й також в межах призначених оперативних умов. Зв'язані з захистом переходи в коді, що управляють поведінкою у виняткових умовах (наприклад, ініціалізація, невдалі тестування функціональності тощо), повинні перевірятися через навмисне створення всіх помилкових станів протягом тестування перевірки достовірності.

2. Має бути в наявності проектне свідоцтво (теоретичне, емпіричне або обидва), що підтверджує всі вимоги захисту ГВБ, включаючи захист від порушення функціонування.

Таким чином, в стандарті, що розглядається, міститься увесь спектр вимог до генераторів випадкових бітів, і, на наш погляд, дані вимоги можуть бути застосовними в Україні.

2. Функціональна модель генератора випадкових бітів

Функціональна модель генератора випадкових бітів, представлена в стандарті ISO/IEC 18031, а також відповідні вимоги та цілі визначають логіку функціонування генераторів випадкових бітів без за-

значення обмежень чи способів. Важливим є те, що дану модель можна застосувати як для недетермінованого, так і для детермінованого ГВБ. Оскільки не всі важливі аспекти генерації випадкових бітів можливо представити алгоритмічно, функціональне представлення генерації випадкових бітів в стандарті ISO/IEC 18031 є центральним для визначення ГВБ.

Функціональна модель, представлена в стандарті ISO/IEC 18031, включає до складу всі компоненти, необхідні для формування випадкових бітів. Цей цілісний підхід є необхідним для гарантії випадковості вихідних даних ГВБ [1].

Дана модель (рис. 1) має шість основних компонентів, проте можливий випадок, коли виконуються всі функціональні вимоги без включення всіх базових компонентів. Цими базовими компонентами є:

- джерело ентропії;
- додаткові вхідні дані;
- внутрішній стан;
- функція переходу внутрішнього стану;
- функція генерації вихідних даних;
- функції підтримки.

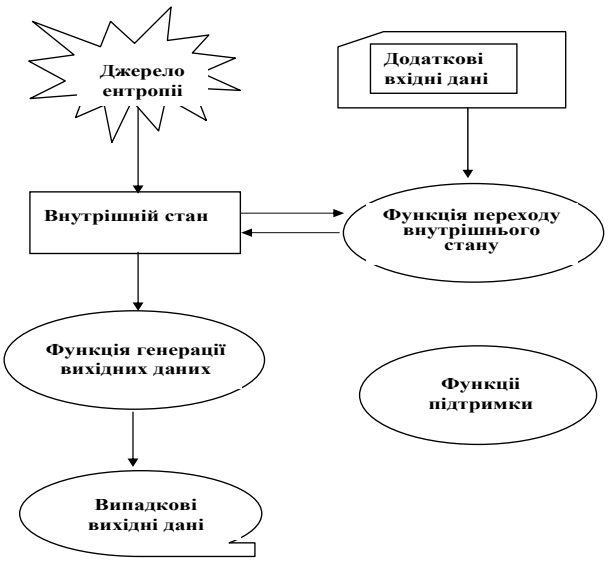

Рис. 1. Функціональна модель генератора випадкових бітів згідно ISO/IEC 18031

3. Експериментальні дослідження властивостей ГВБ

Спираючись на описані в стандарті ISO/IEC 18031 схеми генераторів випадкових бітів було реалізовано генератор випадкових бітів на геш-функціях і перевірено його статистичні характеристики.

У табл. 1 наводяться дані по проходженню псевдовипадковими послідовностями (ПВП) тестів за Правилом 1 [2].

Таблиця 1

Дані по проходженню псевдовипадковими послідовностями тестів за Правилом 1

Генератор	Кількість тестів, у яких тестування пройшли більше 99% послідовностей	Кількість тестів, у яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
ГВБ на геш-функціях	139 (73,54%)	189 (100%)

У табл. 2 представлені зведені результати по проходженню генераторами тестів за Правилом 2 [2].

Таблиця 2

Дані по проходженню псевдовипадковими послідовностями тестів за Правилом 2

Генератор	Кількість тестів, у яких значення ймовірності $P \le 0{,}01$	Кількість тестів, у яких значення ймовірності $P \le 0{,}001$
BBS	0	0
ГВБ на геш-функціях	2	0

Для тестування ГВБ на геш-функціях використовувалася методика NIST STS, рекомендована Національним інститутом по стандартизації й технологіям США, розроблена для статистичного тестування алгоритмів-кандидатів на AES (NIST SP 800-22).

З використанням методики NIST STS було здійснено тестування псевдовипадкової послідовності, а також виконано порівняння властивостей цієї послідовності із властивостями ПВП генератора псевдовипадкових бітів BBS (тестова вибірка, рекомендована NIST).

Як бачимо з результатів, генератор випадкових бітів на базі геш-функцій показав не гірші результа-

ти, ніж визнаний «класичний» генератор BBS. А це є доказом надійності схем генерації, запропонованих в ISO/IEC 18031.

Висновки

Необхідний рівень стійкості криптоперетворень симетричного і асиметричного типу може бути забезпечений тільки при умові, що ключі генеруються випадково або псевдовипадково з необхідними статистичними характеристиками та властивостями ключів. Для виконання цих умов згідно стандарту ISO/IEC 18031 можуть використовуватись два типи генераторів випадкових бітів: недерміновані генератори випадкових бітів та детерміновані генератори випадкових бітів. Гармонізація стандарту генераторів випадкових бітів являється актуальною задачею у зв'язку з широким застосуванням даних технологій в інформаційно-телекомунікаційних системах і необхідністю надати гарантії в правильності реалізації технічних рішень при проектування генераторів випадкових бітів і гарантії, що виконуються спеціальні вимоги, висунуті до властивостей випадкових і псевдовипадкових послідовностей.

Тестування одного генераторів випадкових бітів, що базується на геш-функціях, реалізованого згідно ISO/IEC 18031, підтвердило високий рівень випадковості формуємих ним послідовностей. Генератор випадкових бітів на геш-функціях є достатньо швидкодіючим та має високу стійкість розкриття. Таким чином, генератор на геш-функціях повністю задовольняє вимогам, які пред'являються до генераторів випадкових бітів, і визначені в даному стандарті.

Стандарт ISO/IEC 18031 містить технічні рішення, які відповідають сучасному науково-технічному рівню, не суперечить практичному досвіду розробки і застосування подібних пристроїв.

Література

1. ISO/IEC 18031:2005(E) Information technology – Security techniques – Random bit generation.

2. Потий А.В. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS / А.В. Потий, С.Ю. Орлова, Т.А. Гриненко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вип. 2. – С. 206-214.

Надійшла до редакції 2.02.2009

Рецензент: д-р техн. наук О.В. Потій, Харківський національний університет радіоелектроніки, Харків.

ОБОСНОВАНИЕ ТРЕБОВАНИЙ К ГЕНЕРАТОРАМ СЛУЧАЙНЫХ БИТ СОГЛАСНО ISO/IEC 18031

И.Д. Горбенко, Н.В. Шапочка, А.А. Козулин

В соответствии с существующей нормативно-правовой базой обоснованы и определены требования к генераторам псевдослучайных последовательностей. Определено, что наиболее полно указанным требованиям отвечает стандарт ISO/IEC 18031 «Информационные технологии – Методы защиты – Генерация случайных бит». Предлагается методика и приводится результат исследования основных функциональных моделей генераторов случайных и псевдослучайных бит, которые подтверждают перспективность, возможность и условия применения стандарта ISO/IEC 18031 в Украине.

Ключевые слова*:* генератор случайных битов, случайность, энтропия, статистические свойства, методика статистического тестирования.

THE JUSTIFICATION OF REQUIREMENTS TO RANDOM BIT GENERATORS ACCORDING TO ISO/IEC 18031

I.D. Gorbenko, N.V. Shapochka, O.O. Kozulin

According to existing laws the requirements to pseudorandom sequences generators are proved and determined. It is determined, that the standard ISO/IEC 18031 «Information technology – Security techniques – Random bit generation» corresponds most fully to specified requirements. The technique is offered and the result of research of the basic functional models of generators of random and pseudorandom bits which confirm perspectivity, an opportunity and conditions of application of standard ISO/IEC 18031 in Ukraine is resulted.

Key words*:* random bit generators, randomness, entropy, statistical properties, statistical testing methodology.

Горбенко Іван Дмитрович – д-р техн. наук, проф., зав. кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Харків, Україна.

Шапочка Наталя Вікторівна – аспірантка кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Харків, Україна, e-mail: natali_shap@mail.ru.

Козулін Олексій Олексійович – студент 5-го курсу кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Харків, Україна, e-mail: elxx_kharkov@mail.ru