УДК 004.056.55

ОБҐРУНТУВАННЯ ВИМОГ ТА ВИБІР ЗАСОБІВ ТЕСТУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Д.М. Маковецький
Харківський національний університет радіоелектроніки, м. Харків

Проведено класифікацію та порівняльний аналіз оцінки якості псевдовипадкових послідовностей з довільним алфавітом.

Ключові слова: довільний алфавіт, псевдовипадкова послідовність, генератор псевдовипадкових послідовностей, методика тестування, статистичні тести, функціональні класи.

Вступ. В існуючих криптографічних системах однією з найважливіших складових, яка впливає на криптографічну стійкість і в цілому на безпеку криптографічного захисту інформації, є ключові данні та ключова інформація. На сьогоднішній час загальним підходом до генерування ключів, ключової інформації та параметрів є стандартизація методів, механізмів і практичних (конкретних) алгоритмів їх генерування. Причому, як можна судити із ряду джерел, ці методи, механізми й алгоритми намагаються захистити від розповсюдження особливо в частині генерування випадкових послідовностей. Були розроблені та прийняті спочатку регіональні, а потім і міжнародні стандарти, у яких були визначені вимоги, методи, механізми та алгоритми реалізації генераторів. (ISO/IEC 18031 [1], ANSI X9.82-3 [2], NIST SP 800-90 [3], NIST SP 800-22 [4])), згідно яких до генераторів ключів та ключової інформації висуваються жорсткі вимоги по критеріям нерозрізнюваності, необоротності, швидкодії тощо. Для оцінки вказаних властивостей і характеристик в технічно розвинених державах розроблено ряд нормативних документів та стандартів [1–3], що названі вище. Генератори випадкових послідовностей (чисел) є одними з основних компонентів криптографічних систем. Тільки при використанні ключових даних, сформованих із застосуванням надійних генераторів випадкових чисел (ГВЧ), можуть досягатися заявлені рівні стійкості криптографічного захисту інформації. Такі генератори також формують необхідну для функціонування криптографічних систем ключову інформацію, від якості якої залежить стійкість криптографічних перетворень.

В технологічно розвинених державах питанню обгрунтування вимог до засобів криптографічного захисту інформації приділяється особлива увага. В США починаючи з 90-х років було розроблено та прийнято 3 федеральних стандарти: FIPS 140-1 [5], FIPS 140-2[6] та FIPS 140-3 [7], у Німеччині прийняті нормативні документи (директиви) відповідно для оцінювання ГПВЧ AIS 20 [8] та ГВЧ – AIS 31 [9].

Метою цієї статті є класифікація, порівняний аналіз, обґрунтування та вибір основних нормативних документів та стандартів для оцінки якості псевдовипадкових та випадкових послідовностей. Особливістю постановки цієї задачі є те, що в існуючий базі використовуються методики оцінки, як правило, псевдовипадкових бітів.

Аналіз вимог NIST STS. Набір тестів NIST STS був запропонований у ході проведення конкурсу на новий національний стандарт США блокового шифрування. Цей набір використався для досліджень статистичних властивостей кандидатів на новий блоковий шифр. На сьогодні методика тестування, що запропонована NIST є найбільш поширеною у розробників криптографічних засобів захисту інформації. Порядок тестування окремої двійкової послідовності S згідно NIST STS має такий вигляд [4]: Висувається нульова гіпотеза H_0 – припущення про те, що дана двійкова послідовність S випадкова. За послідовності S розраховується статистика тесту c(S). З використанням спеціальної функції і статистики тесту розраховується значення імовірності $P = f(c(S)),\ P \in [0,1]$. Значення імовірності P порівнюється із рівнем значущості α, $\alpha \in [0.001, 0.01]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається. У противному випадку приймається альтернативна гіпотеза.

Пакет містить у собі 16 статистичних тестів. Але фактично, в залежності від вхідних параметрів обчислюється 189 значень імовірності P, які можна розглядати як результат роботи окремих тестів (у новій версіях 188 значень, необхідно врахувати). Таким чином у результаті тестування двійкової послідовності формується вектор значень імовірності $P = \{P_1, P_2 ... P_{189}\}$. Аналіз складових P_i даного вектору дозволяє вказати на конкретні дефекти випадковості послідовності, що тестується.

Методика тестування NIST STS має такий вигляд.

1. Для кожного апаратного модуля (АМ) необхідно оцінити та прийняти рішення про те, що він формує випадкові двійкові послідовності. Генератор повинен формувати двійкову послідовність $S=\{s_1, s_2, \ldots, s_n\}$, $s_i \in \{0,1\}$ довільної довжини n.

2. Для фіксованого значення n формують множину з m двійкових послідовностей:

$$S_1 = \{s_1, s_2, \ldots, s_n\};$$
$$S_2 = \{s_1, s_2, \ldots, s_n\};$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$S_m = \{s_1, s_2, \ldots, s_n\}.$$

Таким чином, для тестування необхідно сформувати вибірку об'ємом $N = m \times n$.

3. Кожну послідовність перевіряють з використанням пакету NIST STS. У результаті формується статистичний портрет генератора виду

№ теста j / № пос-ті i	1	2	…	q
S_1	$P_{1,1}$	$P_{1,2}$	…	$P_{1,q}$
S_2	$P_{2,1}$	$P_{2,2}$	…	$P_{2,q}$
...	…	…	…	…
S_m	$P_{m,1}$	$P_{m,2}$	…	$P_{m,q}$

$$\Rightarrow \begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1q} \\ P_{21} & P_{22} & \cdots & P_{1q} \\ \vdots & \vdots & \ddots & \vdots \\ P_{m1} & P_{m2} & \cdots & P_{mq} \end{pmatrix}$$

Статистичний портрет генератора задається матрицею розмірністю m×q, де m – кількість двійкових послідовностей, що перевіряються, а q – кількість статистичних тестів, що використовуються для тестування кожної послідовності. Елементи матриці $P_{ij} \in [0,1]$, де $i = \overline{1,m}, j = \overline{1,q}$, представляють собою значення ймовірності, яка отримана у результаті тестування i-ої послідовності j-им тестом.

4. За отриманим статистичним портретом визначають долю послідовностей, що пройшли кожний статистичний тест. Для цього задають рівень значимості $\alpha \in [0.001, 0.01]$ та здійснюють підрахунок значень ймовірностей *P–value*, що перевищують встановлений рівень α для кожного з q тестів, тобто визначають коефіцієнт

$$r_j = \frac{\#\left\{P_{ij} \geq \alpha \middle| i = 1,2,\ldots,m\right\}}{m}. \quad (1)$$

У результаті формується вектор коефіцієнтів $R=\{r_1, r_2, \ldots, r_q\}$, елементи якого характеризують, у відсотках, проходження послідовності S_i всіх статистичних тестів.

Правило 1. Вважається, що генератор G пройшов тестування по j-му тесту, якщо значення коефіцієнту r_j знаходиться в межах довірчого інтервалу [rmax, rmin]. Границі довірчого інтервалу визначаються відповідно виразу

$$r_{\max(\min)} = \hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}}, \quad (2)$$

де $\hat{p} = 1 - \alpha$.

5. Здійснюється статистичний аналіз статистичного портрету. Отримані значення P_{ij} повинні підкорятися рівно ймовірному закону розподілу на інтервалі [0,1]. Для кожного вектору-стовпцю статистичного портрету будується гістограма частостей F_k попадання значень P_{ij} у кожний з k = 1, 2, …, 10 під інтервалів, на які розбитий інтервал [0,1]. Рівноймовірність розподілу значень ймовірностей P_{ij} перевіряється з використанням критерію χ^2. Для цього розраховується статистика виду:

$$\chi_j^2 = \sum_{k=1}^{10} \frac{\left(F_k - m/10\right)^2}{m/10}, \quad (3)$$

яка підкоряється розподілу χ^2 с дев'ятьма ступенями волі.

Правило 2. Вважається, що генератор G пройшов тестування за j-им тестом, якщо виконується умова $\chi_j^2 > 0.0001$.

6. Прикінцеве рішення приймають у відповідності з правилом: вважається, що генератор G пройшов статистичне тестування пакетом NIST STS, якщо значення коефіцієнтів r_j для всіх $j = \overline{1,q}$ знаходяться в межах довірчого інтервалу $[r_{\min}, r_{\max}]$ та виконується умова $\chi_j^2 > 0.0001$ для всіх $j = \overline{1,q}$.

В табл. 1 наведено перелік тестів та інтерпретація результату, який було отримано в ході виконання кожного з тестів, які по суті містять вимоги , що висуваються методикою до випадкових та псевдовипадкових послідовностей.

Таблиця 1

Статистичні тести NIST STS

Статистичний тест	Дефект, що виявляється тестом
Частотний (монобітний тест)	Надто багато нулів або одиниць у послідовності.
Частотний тест (в середині блоку)	Локалізовані відхилення частоти появи одиниць в блоці від ідеального значення 1/2.
Перевірка накопичених сум	Велика кількість одиниць або нулів на початку або наприкінці двійкової послідовності.
Перевірка серій	Надто швидка або надто повільна зміна знака у ході генерації послідовності.
Перевірка максимальної довжини серії у блоці	Відхилення від теоретичного закону розподілення максимальних довжин серій одиниць.
Перевірка рангу двійкової матриці	Відхилення емпіричного закону розподілення значень рангів матриць від теоретичного, що вказує на залежність символів у послідовності.
Спектральний аналіз на основі дискретного перетворення Фур'є	Виявлення періодичних складових (трендів) у двійковій послідовності.
Перевірка шаблонів, що перекриваються	Велика кількість m- бітних серій із одиниць у послідовності.
Універсальний тест Маурера	Залежність та нерівно ймовірність появлення символів.
Ентропійний тест	Нерівномірність розподілення m- бітних слів у послідовності (регулярність властивостей джерела).
Перевірка випадкових відхилень	Відхилення від теоретичного закону розподілення "візитів" у конкретний стан при випадковому блуканні.
Перевірка випадкових відхилень (варіант)	Відхилення від теоретично очікуваної загальної кількості "візитів" при випадковому блуканні у заданий стан.
Послідовний тест	Нерівномірність розподілення m- бітних слів у послідовності.
Перевірка стиснення згідно з алгоритмом Лемпеля–Зива	Великий ступінь стиснення послідовності, що тестується за зрівнянням із ступенем стиснення, що очікується у випадковій послідовності.
Перевірка шаблонів, що не перекриваються	Велика кількість заданих неперіодичних "шаблонів" у послідовності.
Перевірка лінійної складності	Відхилення емпіричного розподілу довжин еквівалентних лінійних рекурентних регістрів для послідовностей фіксованої довжини від теоретичного закону розподілення для випадкової послідовності, що вказує на недостатню складність послідовності, що тестується.

Основним недоліком NIST STS є велика складність методики тестування, що не уможливлює його використання в реальному часі (наприклад, на ПЕВМ з тактовою частотою процесора 750 Мгц проведення комплексного контролю за NIST STS проводиться на протязі 2 годин), тому він рекомендується для використання в наукових дослідженнях та випробуваннях. Але в різних практичних додатках необов'язково використовувати всі 189 тестів. Окремі тести можуть використовуватися і в реальному часі.

Аналіз вимог FIPS 140. Дана методика використовується для технологічного (у процесі функціонування) аналізу вихідних послідовностей генераторів випадкових чисел. У стандартах FIPS PUB 140-1 [5], FIPS PUB 140-2 [6] використовуються чотири основних статистичних тести:

1. *Монобітний тест*. Ціль цього тесту полягає в тому, щоб визначити, чи є число одиничних і нульових біт у послідовності приблизно таким, як очікується для випадкової послідовності. Нехай X і Y позначає кількість нулів і одиниць у послідовності b, відповідно

$$X(Y) = \sum_{j=1}^{20000} b_j \ . \tag{4}$$

Якщо послідовність b1,…,b20000 випадкова, то значення X повинно задовольняти умові 9,725 < X < 10,275. Якщо тест не пройдений, можна зробити висновок, що в послідовності занадто багато нулів або одиниць.

2. *Покер тест*. Для виконання тесту необхідно розділити 20 000-бітовий потік на 5 000 безперервних 4-бітових сегменти. Підрахувати і зберегти число появ 16 можливих 4-бітових значень. Позначити $f(i)$ як число всіх 4-бітових значень i, де $0 < i < 15$. Далі оцінити:

$$X - \left(\frac{16}{5000}\right) * \left(\sum_{i=0}^{15} [f(i)]^2\right) - 5000 \ . \tag{5}$$

Тест вважається пройденим, якщо $2.16 < X < 46.17$.

3. *Тест серій.* Під серією розуміється послідовність однакових символів, тобто послідовність, що складається з послідовних одиниць або нулів. Суть тесту полягає в тому, що на заданій довжині послідовності, яка тестується, здійснюється підрахунок серій довжиною 1, 2, 3, 4, 5, 6 елементів (серії довжиною більш ніж 6 елементів розглядаються як серії довжиною 6).

Метою тесту серій є визначення, чи буде кількість серій одиниць (або нулів) різної довжини у двійковій послідовності такою же, як очікувана у випадкової послідовності. Якщо послідовність випадкова, то кількість серій кожної довжини повинна перебувати в інтервалах, наведених у табл. 2.

Таблиця 2

Допустимі значення для тесту серій залежно від довжини серії

Довжина серії	Необхідний інтервал
1	2,315–2,685
2	1,114–1,386
3	527–723
4	240–384
5	103–209
≥ 6	103–209

4. *Тест довжин серій.* Суть тесту полягає в перевірці максимальної довжини серії з однакових елементів. Якщо послідовність випадкова, то максимальна довжина серії не повинна перевищувати значення 26. (Імовірність події, що полягає в появі серії такої довжини, дуже мала).

Практично перші два стандарти, тобто FIPS PUB 140-1 [5], FIPS PUB 140-2 [6] уже не використовуються. Перспективним є стандарт FIPS 140-3 [7] в якому збільшено число рівнів захисту криптографічних модулів.

В FIPS 140-3, на відміну від FIPS 140-2, врахована необхідність захисту інформації підвищеної конфіденційності, здійснено удосконалення та підсилення вимог, внесені уточнення і виправлення. Також він легко застосовується з новими технологіями. FIPS 140-3 [7] є базовим елементом специфікацій в галузі інформаційної безпеки, включаючи профілі захисту сервісів безпеки та їх комбінацій. В ньому передбачено чотири рівні захисту криптографічних модулів, що дозволяють економічно цілеспрямованим способом захищати дані різної степені критичності в різних умовах. Ці рівні захисту можна розглядати як вимоги до ВП та ПВП.

Сутність вимог зводиться до наступного: використання і безпечна реалізація затверджених функцій безпеки для захисту інформації з обмеженим доступом; забезпечення захисту модуля від несанкціонованого розкриття криптографічних ключів та інших даних, критичних для безпеки; забезпечення захисту модуля від несанкціонованого використання; запобігання несанкціонованій модифікації модуля і криптографічних алгоритмів, в тому числі несанкціонованій модифікації, підміні, вставки та видалення криптографічних ключів та інших даних, критичних для безпеки; забезпечення довіри в тому, що модуль функціонує необхідним чином при роботі в затвердженому режимі; виявлення помилок в функціонуванні модуля і запобігання компрометації інформації з обмеженим доступом і даних модуля, критичних для безпеки внаслідок подібних помилок.

Аналіз вимог AIS 20. У зв'язку з необхідністю використання при розробці технічних рішень спеціальних методів оцінки генераторів псевдо випадкових послідовностей (чисел), які базуються на ряді керівних принципів, у Німеччині прийняті нормативні документи відповідно для оцінки ГВЧ AIS 20 [8] і AIS 31 [9]. При їхній розробці були враховані основні положення й досвід застосування федеральних стандартів США FIPS PUB 140-1 [5] і FIPS PUB 140-2 [6].

В AIS 20 подано критерії, які є вимогами для оцінки детермінованих генераторів випадкових чисел (ДГВЧ). Основна ідея полягає в тому, що придатність ДГВЧ повинна бути оцінена з урахуванням криптографічних додатків, у яких вони використовуються. В AIS 20 вводяться чотири функціональних класи K1, K2, K3, K2, які наведені в табл. 3. Класи функціональності K1–K4 описують набір ієрархічних вимог до ДГВЧ, які виражені на рівні технічних властивостей.

ГВЧ (предмет експертизи) визначається 5-тьма параметрами $(S, R, \varphi, \psi, p_A)$, де S – кінцевий набір можливих внутрішніх станів генератора випадкових чисел; R – набір можливих вихідних значень (випадкові числа); φ (S,S,) – функція стану; ψ (S,R) – функція виходу; p_A – імовірнісна міра, що описує розподіл випадкової величини, яка використовується як початкове число.

Оцінка процесу генерації початкового стану, тобто практичної реалізації розподілу p_A, не є частиною фактичної оцінки ДГВЧ і не входить в оцінні критерії. Однак заявник повинен указати спосіб генерації початкового стану.

Таблиця 3

Функціональні класи AIS 20 [8]

Функціональний клас	Вимоги до ДГВП		Криптографічні додатки , у яких застосовуються ДГВЧ (ДГВБ) відповідного класу
K1	K1(i)	K1 вимагає, щоб послідовність випадкових векторів, що утворена з випадкових чисел з великою ймовірністю була попарно різною	Інтерактивні крипто протоколи встановлення ключів, автентифікації, розподілу таємниці
K2	K1(i)+ K2(ii)	ДГВЧ повинен належати класу K1. K2 d)(ii) вимагає, щоб випадкові числа, які згенеровані ДГВЧ, мали статистичні властивості, подібні до статистичних властивостей випадкових чисел, які згенеровані ідеальним ГВЧ	Симетричні потокові шифри
K3	K1(i)+ K2(ii)+ K3(iii)+ K3(iv)	ДГВЧ повинен належати класу K2. Повинно бути фактично неможливо обчислити або вгадати попереднє r_{i-1} або наступне r_{i+j+1} з відомої підпослідовності $r_i, r_{i+1}, \ldots, r_{i+j}$, $(i + j \le M)$, а також обчислити або вгадати внутрішній стан	Генерація ключів сеансу цифрового підпису чи направленого шифрування (секретний ключ *x* або випадкове число *k DSS, EC DSS*), генерація паролів. тощо.
K4	K1(i)+ K2(ii)+ K3(iii)+ K3(iv)+ K4(v)	ДГВЧ повинен належати класу K3. K4 d)(v) Повинно бути фактично неможливо виробити попереднє випадкове число ri-1 знаючи внутрішній стан si	Генерація ключів сеансу цифрового підпису чи направленого шифрування (секретний ключ *x* або випадкове число *k DSS, EC DSS*), генерація паролів, генерація ключів сеансу для симетричних криптографічних механізмів тощо.

Заявник повинен надати експертові такі данні: призначення функціонального класу (K1, K2, K3, K4) і призначення стійкості механізму (“висока”, ”середня”, ”низька”); закінчений і ясний неофіційний опис ДГВЧ; визначальні параметри (S, R, ϕ, ψ, p_A); верхню границю M для максимального числа випадкових чисел, які можуть бути згенеровані ДГВЧ за його повний експлуатаційний цикл або поки він заново не буде ініційований з новим початковим станом $s_0 \in S$; чіткий опис способу генерації початкового стану; додаткову інформацію (при необхідності).

В AIS 20 [8] для верифікації вимог використовуються п’ять основних статистичних тестів T1–T5:

1) монобітний тест – метою цього тесту полягає в тому, щоб визначити, чи є число одиничних і нульових біт у послідовності приблизно таким, як очікується для випадкової послідовності;
2) покер тест – метою покер тесту є визначення, чи будуть блоки довжиною m зустрічатися в послідовності b з такою же частотою, як у випадковій послідовності;
3) тест серій – метою тесту серій є визначення, чи буде кількість серій одиниць (або нулів) різної довжини у двійковій послідовності такою же, як очікувана у випадкової послідовності;
4) тест довжин серій – суть тесту полягає в перевірці максимальної довжини серії з однакових елементів;
5) автокореляційний тест – тест розраховує кореляцію між бітами послідовності та її зсувами (метою тесту є перевірка кореляції між послідовністю та її не циклічними зсувами).

Для проведення технологічного тестування необхідно згенерувати випадкову послідовність b довжиною n=20000 бітів. В якості нульової гіпотези H_0 передбачається, що послідовність випадкових чисел, яка тестується, видається ідеальним джерелом шуму. Якщо припустити, що послідовності $b_1, \ldots, b_{20000}$ або $w_1, \ldots, w_{2\text{^}16}$ – вихід ідеального джерела шуму, то ймовірність відхилення нульової гіпотези для кожного з тестів T1–T5 $\approx 10^{-6}$.

Методика, що визначена в AIS 20 [8] використовується для тестування детермінованих псевдовипадкових послідовностей. В залежності від вимог, що висуваються до ДГВЧ, можуть застосовуватися чотири рівні вимог перевіряння псевдовипадкових чисел на випадковість K1–K2. Методика тестування AIS 20 може застосовуватись як в реальному часі, так і в процесі досліджень, та для технологічного тестування.

Аналіз вимог AIS 31. В AIS 31 [9] представлені критерії оцінки криптографічних властивостей генераторів випадкових чисел. Аналіз показав, що AIS 31 базується на математично-технічній основі BSI AIS 20 [8]. Оцінка фізичних генераторів випадкових чисел (ФГВЧ) грунтується в основному на статистичних тестах. На основі різних можливих сценаріїв атак можна розробити вимоги до властивостей зовнішніх і відповідно внутрішніх випадкових чисел. Беручи до уваги ці обставини в AIS 31 уведені 2 класи функціональності (P1, P2) [9]. Що стосується застосування, то класи P1 і P2 власне кажучи відпо-

відають класам К1–К2 і К3–К4 AIS 20 [8]. В AIS 31 враховані вимоги якісного перевіряння на випадковість та можливості оперативного тестування. Перевірка здійснюється на відповідність функціональним класам Р1 та Р2. При перевірці на відповідність Р1 використовуються тести, що були взяті в FIPS 140-1 [5], але додатково введено автокореляційний тест, що дозволяє перевірити кореляції між послідовністю та зсувами цієї ж послідовності. При перевірці на відповідність до Р2 додатково використовуються три тести: тест перевірки рівномірного закону розподілу, порівняльний тест для поліноміальних розподілів та ентропійний тест [9]. Властивість Р1 вимагає статистичної відмінності внутрішніх випадкових чисел. Р2 клас вимагає, щоб було практично неможливо визначити випадкове число, навіть якщо його попередні або наступні елементи відомі. Клас Р2 є найвищим можливим класом у межах технічних вимог BSI AIS 31 [9].

Для відповідності класу Р1 повинні виконуватися вимоги P.1d)(i)-P1.d)(vi) відповідно до механізмів і функцій стійкості [9].

P.1d)(i) вимагає, щоб послідовність випадкових векторів, утворена із внутрішніх випадкових чисел $r_1, r_2, \ldots$ із великою ймовірністю була попарно різною (тест Т0).

Для верифікації вимоги P.1d)(ii) внутрішні послідовності ВЧ $r_1, r_2, \ldots$ й їхні проекції на окремі біти повинні задовольняти статистичним тестам Т1–Т5, що наведені нижче.

P.1d)(iii) (якщо стійкість механізмів або функцій "середня" або "висока"). Якщо при включенні ФГВЧ відбувається загальна зупинка джерела шуму, то ця зупинка повинна бути негайно ж розпізнана, і після зупинки випадкові числа не можуть видаватись на зовні.

P.1d)(iv) (якщо стійкість механізмів або функцій "середня" або "висока"). Якщо під час роботи ФГВЧ виникає загальна зупинка джерела шуму, то після неї припиняється виробка випадкових чисел. В якості заміни досить, щоб після загальної зупинки джерела шуму ФГВЧ функціонував для кожної однакової послідовності сигналів шуму згідно вимог К2-ДГВЧ AIS 20, вихідні послідовності якого відповідають передбаченій меті застосування.

P.1d)(v) (якщо стійкість механізмів або функцій повинна бути "висока"). Необхідні в P.1d)(i) і P.1d)(ii) властивості повинні бути верифіковані при передбачених зовнішніх впливах (t0, електропостачання й т.д.), тому що вони можуть впливати на функціонування джерела шуму.

P.1d)(vi) (якщо стійкість механізмів або функцій "середня" або "висока"). ФГВЧ повинен містити online-тест, який по зовнішньому виклику перевіряє якість внутрішніх випадкових чисел [9].

Вимоги на відповідність ФГВЧ класу Р2 [9].

ФГВЧ повинен належати класу Р1 як мінімум з такими ж механізмами і функціями стійкості.

P2.d)(i)-P2.d)(vi). Верифікація властивостей Р1.

P2.d)(vii). Дискретизовані послідовності шумових сигналів (ДПШС), що задовольняють певним критеріям, повинні проходити статистичні тести, які крім усього іншого повинні виключити багатокрокові залежності. Крім того, повинен бути пройдений ентропійний тест Т8.

P2.d)(viii). Додаткова математична обробка не повинна зменшувати ентропію на біт.

P2.d)(ix) (якщо стійкість механізмів або функцій "середня" або "висока"). При кожному включенні ФГВЧ повинні бути засвідчені мінімальні статистичні властивості ДПШС. Доти, поки не закінчиться статистичне тестування, випадкові числа не можуть бути видані.

P2.d)(x) (якщо стійкість механізмів або функцій "середня" або "висока"). Якщо під час роботи ФГВЧ відбувся загальний останов джерела шуму, повинна виключатися видача випадкових чисел, тому що відповідні внутрішні випадкові послідовності були генеровані після зупинки.

P2.d)(xi) (якщо стійкість механізмів або функцій "середня" або "висока"). У роботу ФГВЧ повинен бути імплементовано online-тест, за допомогою якого може бути перевірена статистична якість дискретизованої послідовності шумового сигналу. Online-тест повинен бути викликаним ззовні або ж ФГВЧ повинен сам викликати його. Останнє повинне здійснюватися постійно або принаймні через регулярні проміжки. Online-тест повинен розпізнати в погоджений час незначні статистичні дефекти або погіршення статистичних властивостей дискретизованої шумової послідовності.

P2.d)(xii) (якщо стійкість механізмів або функцій "висока"). Необхідні в P2.d)(vii) властивості повинні бути верифіковані для передбачених зовнішніх умов застосування (t^0, енергопостачання й т.д.), тому що вони можуть впливати на функціонування джерела шуму.

P2.d)(xiii) (якщо стійкість механізмів або функцій "висока"). ФГВЧ повинен сам викликати online-тест.

В AIS 31 для верифікації вимог P1.d)(i), (ii), (v) і P2.d(vii) і (xii) використовуються тести Т0–Т8, що наведені нижче [9]:

Т0 – диз'юнктивний тест – при його виконанні здійснюється перевірка, що в множині, що формується з слів не існує жодного послідовного однакового слова;

Т1 – монобітний тест – мета цього тесту полягає в тому, щоб визначити, чи є число одиничних і нульових біт у послідовності приблизно таким, як очікується для випадкової послідовності;

Т2 – покер тест – метою тесту серій є визначення, чи буде кількість серій одиниць (або нулів) різної довжини у двійковій послідовності такою же, як очікувана у випадкової послідовності;

Т3 – тест серій – метою тесту серій є визначення, чи буде кількість серій одиниць (або нулів) різної довжини у двійковій послідовності такою ж, як очікувана у випадкової послідовності;

Т4 – тест довжин серій – суть тесту полягає в перевірці максимальної довжини серії з однакових елементів;

Т5 – автокореляційний тест – при виконанні цього тесту розраховується кореляція між бітами послідовності та її зсувами. Метою тесту є перевірка кореляції між послідовністю та її не циклічними зсувами;

Т6 – тест перевірки рівномірного закону розподілу – тест дозволяє перевірити чи виконується монобітний тест на послідовностях $k \le n$;

Т7 – порівняльний тест для поліноміальних розподілів – для кожного $i \in \{1,\ldots,h\}$ беруть n-елементну вибірку значень $w_{i1},\ldots,w_{in}$ з множини $\{0,1,\ldots,s\text{-}1\}$. Нульова гіпотеза говорить про те, що поліноміальний розподіл окремих вибірок, що лежать в основі, ідентичний;

Т8 – ентропійний тест – ентропійний тест проводиться згідно Coron. Статистика ентропійного тесту – міра погодженості спостережуваного значення ентропії джерела з тим, що теоретично очікується для випадкового джерела.

Для верифікації Р1 застосовуються тести Т0–Т5 [7]. Властивості Р1.d)(i) і (ii) є відносно слабкими й повинні бути задоволені майже для всіх фізичних джерел шуму. В якості нульової гіпотези H_0 передбачається, що послідовність випадкових чисел, що тестується, видається ідеальним джерелом шуму. Тести Т0–Т5 застосовуються для внутрішніх випадкових чисел. Якщо припустити, що послідовності $w_1,\ldots,w_{2\text{^}16}$ або $b_1,\ldots,b_{20000}$ – вихід ідеального джерела шуму, то ймовірність відхилення нульової гіпотези для тесту Т0 $\approx 2^{-17}$ і для тестів Т1–Т5 $\approx 10^{-6.}$

З метою верифікації Р2 застосовуються додатково тести Т6–Т8 [9]. Тести Т6–Т8 застосовуються до дискретних значень послідовностей шумових сигналів. Припускаючи, що послідовності $w_1,\ldots,w_n$ або $b_1,\ldots,b_{(Q+K)L}$ видаються ідеальним джерелом шуму, імовірності відхилення при обраних у Р2.i) параметрах зневажливо малі. Це пов'язано з тим, що дискретизовані послідовності шумових сигналів реального ФГВЧ завжди мають статистичні дефекти (залежності й т.д.), границі відхилень вибирають так, щоб ФГВЧ із припустимими слабостями пройшли б ці тести. Для проведення технологічного тестування необхідно згенерувати апаратним ГВЧ випадкову послідовність b довжиною n = 20000 біт. Попередні дослідження та тестування підтвердили, що AIS 31 [9] є надійним механізмом тестування і по своїй ефективності забезпечує практично ті ж результати, що і NIST STS [4]. Перевагою AIS 31 є те, що він забезпечує тестування в реальному часі.

Аналіз вимог ДСТУ ISO/IEC 19790. Особливістю ДСТУ ISO/IEC 19790 є те що якщо в криптографічному модулі застосовуються затверджені механізми генерування випадкових бітів та в затвердженому режимі операцій, то модуль повинен виконувати наступне суцільне тестування генератора випадкових бітів [10].

1. Якщо кожний виклик до ГВЧ створює n-бітові блоки (де n > 15), то перший n-бітовий блок, що генерується після включення або ініціалізації, не повинен використовуватися, а повинен зберігатися для порівняння з наступним n-бітовим блоком, що генерується. Кожна наступна генерація n-бітового блоку повинна порівнюватися з блоком, згенерованим раніше. Тестування вважається невдалим, якщо будь-які два порівнювані n-бітових блоки рівні.

2. Якщо кожний виклик до ГВЧ створює менше 16 бітів, то перші n бітів, що генеруються після включення або ініціалізації (для деякого n > 15) не повинні використовуватися, а повинні зберігатися для порівняння з наступними n бітами, що генеруються. Кожна подальша генерація n бітів повинна порівнюватися з n бітами, які були згенеровані раніше. Тестування вважається невдалим, якщо рівні будь-які дві порівнювані n-бітові послідовності . Слід зазначити, що це тестування призначено тільки для тестування мінімальної функціональності генератора випадкових бітів і не пов'язано з якістю випадкової генерації .

Висновки. Із наведеного вище можна зробити висновок, що від якості випадковості формування ключів, ключової інформації та системних параметрів суттєво залежить криптографічна стійкість. ГВП та ГПВП є важливішими складовими елементами криптографічних систем ключових даних і ключової інформації, від якості якої залежить стійкість криптографічних перетворень. Одним із важливих і необхідних напрямків досліджень і створення ефективних ГВП та ГПВП є розробка методів і оцінки статистичних властивостей випадкових послідовностей. Статистичні показники мають вагомий вплив на загальну оцінку ефективності ГВЧ. По суті, статистичні показники та побудовані на їх основі критерії оцінки є інструментом перевірки правильності технічних рішень щодо побудови ГВП [4–10].

1. Результатом проведеного аналізу існуючих методик статистичного тестування генераторів випадкових послідовностей показали, що на цей час найбільш доведеними та практичними до використання методиками є методики NIST STS, FIPS PUB 140 – 3, AIS 20 та AIS 31.

2. Методика FIPS PUB 140-3 може застосовуватись як засіб оперативного контролю, що обумовлено високою швидкодією виконання статистичного тестування. Використання цієї методики дозволяє здійснювати статистичний контроль під час функціонування ГВЧ. Додатковою причиною використання цієї методики є те, що вона є стандартом для контролю криптографічних модулів.

3. Методика NIST STS може застосовуватись як засіб комплексного контролю. Обрання методики обумовлено тим, що вона містить необхідний набір статистичних тестів, сукупність яких обгрунтована, пропонує критерії прийняття рішення відносно не тільки окремої послідовності, але і відносно всього ГВЧ. Додатковим фактором обрання методики є позитивний досвід її використання при дослідженні статистичних властивостей алгоритмів блочного та поточного шифрування, що висовувались на національний стандарт США та держав ЕС.

4. Методика, що визначена в AIS 20 використовується для тестування детермінованих псевдовипадкових послідовностей. Може застосовуватись як в реальному часі, так і в процесі досліджень, та для технологічного тестування.

5. Попередні дослідження та тестування підтвердили, що AIS 31 є надійною методикою тестування і по своїй ефективності забезпечує результати, що і NIST STS. Перевагою AIS 31 є те, що він забезпечує тестування в реальному часі. Методика, що визначена в AIS 31, може застосуватися як в реальному часі, так і в процесі досліджень, та для технологічного тестування. В AIS 31 враховані вимоги якісного перевіряння на випадковість та можливості оперативного тестування.

РЕЗЮМЕ

Проведена классификация и сравнительный анализ обоснования и выбора документов и стандартов для оценки качества псевдослучайных последовательностей.

Ключевые слова: псевдослучайная последовательность, генератор случайных последовательностей, методика тестирования, статистические тесты, функциональные классы.

SUMMARY

Classification and comparative analysis was held of the justification and choice of documents and standards for assessing the quality of pseudorandom sequences.

Keywords: pseudorandom sequence, generator of random sequences, method of testing, statistical tests, functional classes.

СПИСОК ЛІТЕРАТУРИ

1. ISO/IEC 18031 Information technology – Security techniques – Random bit generation. 2005.
2. Стандарт ANSI.X9/17.
3. NIST SP 800-90. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. June 2006.
4. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: [Електронний ресурс]. April 2000. – Режим доступу: http://csrc.nist.gov /publications/nistpubs//SP800-22rev1a.pdf.
5. Federal Information Processing Standards Publication (FIPS PUB) 140 – 1. Security requirements for cryptographic modules. NIST, 1994.
6. Federal Information Processing Standards Publication (FIPS PUB) 140 – 2. Security requirements for cryptographic modules. NIST, 1999.
7. National Institute of Standards and Technology, FIPS 140 – 3 (DRAFT), Security requirements for cryptographic modules: [Електронний ресурс]. – Режим доступу: http://www. nist.gov/cmvp.
8. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for Deterministic random number generator. 1999.
9. Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generator. 2001. Certifications body of the BSI in context of certifications scheme. BSI, 2001. – 38 p.
10. ISO/IEC FCD 19790: Information technology – Security requirements for cryptographic modules. Project: 1.27.40.

Надійшло до редакції 16.09.2013 р.