Захист інформації

УДК 004.056

О.А. Замула[1], Д.О. Семченко[2], Ю.В Землянко[3]

[1] *Харківський національний університет імені В.Н. Каразіна, Харків*
[2] *Харківський національний університет радіоелектроніки, Харків*
[3] *Харківський державний університет харчування та торгівлі, Харків*

АНАЛІЗ І ОБҐРУНТУВАННЯ КРИТЕРІЇВ І ПОКАЗНИКІВ ЕФЕКТИВНОСТІ КРИПТОГРАФІЧНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

*Наведений аналіз вимог до побудови систем криптографічного захисту інформації. Розглянут*і *методики оцінки статистичних властивостей псевдовипадкових послідовностей. Надані рекомендації з використання кожної з розглянутих методик. Вказані необхідні і достатні умови для створення криптографічно-стійких генераторів на підставі міжнародних та національних стандартів. Запропоновано підходи щодо визначення рівнів гарантій криптографічно-стійких генераторів псевдовипадкових послідовностей.*

Ключові слова: *генератор, методика, стандарт, рівень гарантій, FIPS PUB 140-1, NIST STS, AIS 20, AIS 31.*

Вступ

Постановка задачі. Сучасний етап розвитку більшості з компаній характеризується зростаючою роллю інформаційно-телекомунікаційних систем (ІТС) та широким впровадженням інформаційних технологій в усі сфери їх життєдіяльності, підвищення ефективності управління компанією. Збільшення обсягів та різнобічність інформації, що обробляється в інформаційних системах (ІС) компаній, необхідність обробки інформації з обмеженим доступом та розмежування повноважень, територіальна розгалуженість інформаційних та телекомунікаційних систем та інші фактори призводять до зростання потенційних можливостей порушення конфіденційності, цілісності і доступності інформації та системних ресурсів, негативного впливу на інформаційні ресурси та функціонування ІТС.

Витік та викривлення інформації, що складає державну або іншу, передбачену законом таємницю, а також конфіденційної інформації, що є власністю компаній – суттєві потенційні загрози безпеці інформації компаній.

Аналіз наукових досліджень. Проведений аналіз [1 – 4] показав, що ефективним механізмом забезпечення захисту інформації є криптографічне перетворення інформації. На криптографічний захист покладається вирішення завдань запобігання несанкціонованого доступу (НСД) до інформації та системних ресурсів. Загальновизнаним є той факт, що необхідна якість криптографічного захисту забезпечується тільки при використанні спеціальних засобів криптографічного захисту інформації:

- апаратних, програмних, програмно-апаратних засобів, що реалізують криптографічне перетворення інформації;
- апаратних, програмних, програмно-апаратних засобів забезпечення цілісності та справжності інформації, у тому числі засобів імітозахисту та цифрового підпису, що здійснюються за допомогою криптографічного перетворення інформації;
- апаратних, програмних, програмно-апаратних засобів, призначених для управління ключовими даними, включаючи генерацію ключових даних та виготовлення ключових документів;
- апаратних, програмних та програмно-апаратних засобів захисту інформації від НСД, що використовують криптографічні алгоритми перетворення інформації.

Однією з основних умов забезпечення необхідного рівня гарантій криптографічної стійкості захисту є застосування ключових даних і відповідне управління ключовими даними та ключовою інформацією [3]. У свою чергу рівень гарантій криптографічної стійкості дозволяє надавати з необхідною якістю такі базові послуги, як конфіденційність, цілісність, автентичність (справжність).

Криптографічна стійкість криптографічних перетворень і безпечність реалізації різноманітних криптографічних протоколів суттєвою мірою залежить від того, яким чином генеруються та застосовуються різні види ключових даних (ключів) [3 – 7]. Загальним підходом до генерування ключів є застосування для цього генераторів випадкових послідовностей (ГВП) та/або детермінованих генераторів випадкових послідовностей (ДГВП) [5 – 9].

Завдання розроблення генераторів псевдовипадкових чисел (ВП) для криптографічних додатків полягає у розробці доказово стійких методів формування ПВЧ, реалізація яких задовольняє системі обмежень на окремі показники ефективності.

До генераторів випадкових послідовностей і детермінованих генераторів випадкових послідовностей (бітів) висуваються складні вимоги щодо генерування символів послідовності.

Властивості ГВП оцінюють з використанням ряду кількісних показників [3], основними з яких є:

- період l (довжина) ПВП;
- основа алфавіту m;
- ймовірність перекриття в просторі або в часі двох сегментів Y_r та Y_μ, тобто в різних абонентів або в одного абонента протягом часу, так, що $Y_r = Y_\mu$;
- структурна скритність (еквівалентна складність) S_e послідовності Y;

кількість (ентропія $N_k(H_k)$ джерела) ключів для випадку, коли генератор ВП використовується як джерело ключів;

- відстань рівнозначності ℓ_0 конкретної послідовності Y_v;
- безпечний час ГВЧ t_b;
- складність I_y формування послідовності Y;
- довжина параметрів зворотного зв'язку;
- властивості випадковості, рівноймовірності, незалежності та однорідності.

За всіма названими показниками до генератора ПВП повинен бути пред'явлений ряд вимог [3]. Так період повторення $\ell_n \geq \ell_z$, тобто повинен бути не менше заданого, можливість змінної основи алфавіту m, ймовірність перекриття $P_n < P_z$ менше допустимої, структурна скритність $S \geq S_g$, ентропія джерела ключів $H \geq H_g$, відстань рівнозначності $\ell_0 > \ell_g$, безпечний час $t_b > t_g$, тобто не менш допустимих. Крім того, реалізації Y_i повинна задовольняти вимогам випадковості, рівноймовірності, незалежності та однозначності.

Загальним підходом до генерування ключів, ключової інформації та параметрів є стандартизація методів, механізмів і практичних (конкретних) алгоритмів їх генерування.

На теперішній час розроблені та прийняті регіональні і міжнародні стандарти [5 – 11], у яких визначені вимоги, методи, механізми та алгоритми реалізації генераторів. Оскільки при застосуванні засобів криптографічного захисту інформації необхідністю є відновлення ключів та ключової інформації у просторі й часі, у зазначених стандартах розглядаються тільки детерміновані генератори випадкових бітів.

Базовими міжнародними стандартами, що стандартизують алгоритми генерації послідовностей випадкових чисел є [9, 10]:

- міжнародний стандарт ISO/IEC 18031 “Information technology – Random number generation”, який визначає алгоритми генерації псевдовипадкових і випадкових чисел, а також визначає статистичні тести перевірки генераторів;
- міжнародний стандарт ISO/IEC 18032 “Information technology – Prime number generation”, який визначає методи генерації простих чисел і методи тестування чисел на простоту;
- національний стандарт ДСТУ ISO/IEC19790 «Інформаційна технологія – Методи захисту – Вимоги щодо захисту для криптографічних модулів».

Додаткові вимоги до алгоритмів та реалізацій методів і засобів генерації та тестування послідовностей випадкових чисел визначаються національними та промисловими стандартами США – FIPS 140-3, ANSI X9.17, ANSI X9.31, ANSI X9.44 та ін., а також рекомендаціями NIST – NIST SP 800-22 [11] і рекомендаціями органу зі стандартизації Німеччини – AIS-20 [5], AIS-31 [6] та ін.

Одним із важливих та необхідних напрямків досліджень при створенні ефективних генераторів випадкових чисел та генераторів псевдовипадкових чисел є розробка методів та засобів оцінки статистичних властивостей випадкових послідовностей. Статистичні показники та побудовані на їх основі критеріїв оцінки є інструментом перевірки правильності технічних рішень щодо побудови ГВЧ. Дослідження статистичних властивостей здійснюються у рамках методики статистичних випробувань на основі статистичних тестів.

Найбільш прийнятними (з точки зору практичного використання) методиками тестування є методики NIST STS, FIPS PUB 140-1, AIS 20 та AIS 31 [11, 8, 5, 6]. Розглянемо їх детально спочатку питання щодо їх застосування, а потім сутність деяких з них.

Основна частина

1. Застосування методик оцінки статистичних властивостей випадкових послідовностей

Методика FIPS PUB 140-1 – застосовується як засіб оперативного контролю. Її застосування обумовлене високою швидкодією виконання статистичного тестування і дозволяє здійснювати статистичний контроль під час функціонування генераторів випадкових чисел. Додатковою причиною використання цієї методики є те, що вона є стандартом для контролю криптографічних модулів. Методика FIPS 140-1 містить чотири основних статистичних тести [4]. По результатам проходження цих тестів приймається рішення про випадковість послідовності.

Методика NIST STS – застосовується як засіб комплексного контролю. Вибір цієї методики зумовлений тим, що вона містить необхідний набір статистичних тестів, сукупність яких обґрунтована, про-

понує критерії прийняття рішення відносно не тільки окремої послідовності, але й відносно всього ГВБ. Методика статистичного тестування NIST STS налічує 16 статистичних тестів, які дозволяють з великою мірою довіри відбракувати послідовності, які не відповідають вимогам випадковості.

Методика, що визначена в AIS 20, – використовується для тестування детермінованих випадкових послідовностей. Може застосовуватись як у реальному часі, так і в процесі досліджень, а також для технологічного тестування. Методика налічує 5 статистичних тестів представляє критерії 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 [3].

Методика, визначена в AIS 31, є надійною методикою тестування і за своєю ефективністю забезпечує такі самі результати, що й NIST STS. Методика, визначена в AIS 31, може застосуватися як у реальному часі, так і в процесі досліджень, а також для технологічного тестування. В AIS 31 враховані вимоги якісної перевірки на випадковість і можливості оперативного тестування. В AIS 31 [6] представлені критерії оцінки криптографічних властивостей генераторів випадкових чисел, які базуються на математично-технічній основі AIS 20. Оцінка фізичних генераторів випадкових чисел (ФГВЧ) ґрунтується в основному на статистичних тестах. На основі різних можливих сценаріїв атак розробляються вимоги до властивостей зовнішніх і відповідно внутрішніх випадкових чисел. Методика налічує 8 статистичних тестів.

2. Сутність методик тестування випадкових послідовностей

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

ДГВЧ (предмет експертизи) визначається 5-ма параметрами (S, R, φ, ψ, 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 – ймовірнісна 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 має вказати спосіб генерації початкового стану.

Заявник повинен надати експертові такі дані:

- 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 межу 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 (за необхідності).

Вимоги на відповідність ДГВЧ класу K1 [5].

K1(I) вимагає, щоб послідовність випадкових векторів $(r_1,\ldots,r_c)$, $(r_{c+1},\ldots,r_{2c})$, …, $(r_{M-c+1},\ldots,r_M)$, що утворена з випадкових чисел (ВЧ) r_1, r_2, … з великою ймовірністю була попарно різною. Імовірність того, що вектори $(r_1,\ldots,r_c)$, $(r_{c+1},\ldots,r_{2c})$, …, $(r_{M-c+1},\ldots,r_M)$попарно різні, має бути принаймні 1 – ε.

Якщо ε = 0, то стійкість механізму заявляється «висока».

В інших випадках застосовується таке:

$M^2/\left(c^2\varepsilon\right) > 2^{52}$ і $\varepsilon < 2^{-16}$– стійкість механізму заявляється «висока»;

$M^2/\left(c^2\varepsilon\right) > 2^{32}$ і $\varepsilon < 2^{-12}$ – стійкість механізму заявляється «середня»;

$M^2/\left(c^2\varepsilon\right) > 2^{20}$– стійкість механізму заявляється «низька».

Вибір параметрів c, ε, і M залежить від призначення застосування й розрядності випадкових чисел, що генеруються ДГВЧ ($c \in N$ і $\varepsilon \in [0, 1]$).

Логічне зусилля, що необхідне для атак повторення, які спрямовані на визначення параметрів (S, R, φ, ψ, p_A), строго монотонно залежить від зменшення ε, і якщо c фіксоване – строго монотонно від збільшення M.

Вимоги на відповідність ДГВЧ класу K2 [5].

ДГВЧ має належати класу K1.

K2 (II) вимагає, щоб випадкові числа (ВЧ), які згенеровані ДГВЧ, мали статистичні властивості, подібні до статистичних властивостей випадкових чисел, що згенеровані ідеальним ГВЧ. Для верифікації вимоги K2 (II) послідовності ВЧ r_1, r_2, … та їхні проекції на окремі біти мають задовольняти відповідним статистичним тестам, що наведені в опису методики AIS 20. Стійкість механізму, що відповідає K2, є частиною специфікації K1.

Оцінка результатів тестів не залежить від стійкості механізму.

Статистичні тести мають бути досить сильними, щоб виключити відомі атаки на криптографічні алгоритми, що засновані на статистичних слабкостях випадкових чисел [5].

Вирішальне правило [5]. Якщо ДГВЧ проходить всі індивідуальні тести, тоді підтверджується, що ДГВЧ задовольняє вимозі К2 (II) . Якщо більш ніж один індивідуальний тест не пройдено, то вважають, що ДГВЧ не задовольняє вимозі К2 (II).

Якщо тільки один тест не пройдено, то весь порядок тестування має бути повторено, і якщо на цей раз ДГВЧ проходить всі тести, то підтверджується, що він задовольняє вимозі К2 (II). Друге повторення тестування не дозволяється [5].

Підтверджується, що ДГВЧ задовольняє вимогам класу К2, якщо він визначений як К1 ДГВЧ і проходить тести для К2 відповідно до вирішального правила.

Метою К2 є виключення кореляційних атак на криптографічні алгоритми, що засновані на використанні статистично слабких ВЧ (можливо в якості випадкових ключів).

Вимоги на відповідність ДГВЧ класу К3 [6]

ДГВЧ має належати класу К2.

К3(III). Якщо стійкість механізму «висока», то $H(p) \geq 80$; для «середньої» стійкості механізму – $H(p) \geq 48$. Ентропія p_A обчислюється як

$$H(p) = -\sum_{s \in S} p_A(s) \cdot \log_2\left(p_A(s)\right).$$

К3(IV) має бути фактично неможливо обчислити або вгадати попереднє r_i-1 або наступне r_i+j+1 з відомої підпослідовності r_i, r_i+1, …, r_i+j, (i + j ≤ M)), а також обчислити або вгадати внутрішній стан. Потенціал передбачуваних атак супротивника залежить від стійкості механізму. Навіть використовуючи сучасні передові знання, імовірність атаки (реалізована прийнятним частковим методом перебору) може бути незначно більше чим, якби підпослідовність була би не відомою. Передбачається, що супротивник знає параметри (S, R, φ, ψ, p_A), однак він не знає ніяких внутрішніх станів $s_0, s_1, \ldots, s_M$.

При підтвердженні приналежності до К3 зі стійкістю механізму «висока» («середня»), властивості III, II і I (див. К1.I) мають бути оцінені зі стійкістю механізму «висока» («середня»).

Метою К3 є захист проти відновлення попередніх випадкових чисел і вгадування наступних з відомої підпослідовності.

Вимоги на відповідність ДГВЧ класу К4.

ДГВЧ має належати класу К3.

К4 (V) має бути фактично неможливо виробити попереднє випадкове число r_i-1, знаючи внутрішній стан s_i. Потенціал передбачуваних атак супротивника залежить тут від стійкості механізму. Навіть використовуючи сучасні передові знання, імовірність атаки (реалізована прийнятним частковим методом перебору) може бути незначно більшою, ніж якби s_i було б не відоме. Передбачається, що супротивник знає параметри (S, R, φ, ψ, p_A).

Вимога V захищає не тільки безпосередньо попереднє r_{i-1}-му випадкове число, але й кожне r_v і s_v, де v< i. Вимога V є більш жорсткою версією IV, оскільки якщо внутрішній стан si відомий, то можна легко обчислити випадкові числа r_i, …, r_{i+j}.

При підтвердженні приналежності до К4 зі стійкістю механізму «висока» («середня»), не тільки властивість V має бути оцінена зі стійкістю механізму «висока» («середня»), але також і властивість I (див. К1)), III і IV (див. К3).

Метою К4 є захист проти відновлення попередніх випадкових чисел з відомого внутрішнього стану.

В AIS 20 для верифікації вимог К2 використовуються п’ять основних статистичних тестів, які наведені в опису методики.

Тести, разом із позначеннями й межами відхилень, узяті з FIPS PUB 140-1.

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, …, b_{20000} або w_1, …, $w_{2\uparrow 16}$ – вихід ідеального джерела шуму, то ймовірність відхилення нульової гіпотези для кожного з тестів складає приблизно 10-6.

Методика, що визначена в AIS 20, використовується для тестування детермінованих псевдовипадкових послідовностей. Залежно від вимог, що висуваються до ДГВЧ, можуть застосовуватися чотири рівні вимог перевіряння псевдовипадкових чисел (ПВЧ) на випадковість К1-К2. Методика тестування AIS 20 може застосовуватись як в реальному часі, так і в процесі досліджень, а також для технологічного тестування.

Пропозиції щодо використання вимог AIS 31.

В AIS 31 [6] подані критерії оцінки криптографічних властивостей генераторів випадкових чисел. Аналіз показав, що AIS 31 базується на математично-технічній основі AIS 20.

Оцінка фізичних генераторів випадкових чисел (ФГВЧ) ґрунтується в основному на статистичних тестах.

На основі різних можливих сценаріїв атак можна розробити вимоги до властивостей зовнішніх і відповідно внутрішніх випадкових чисел. В AIS 31 введені 2 класи функціональності (P1, P2). Щодо застосування, то класи P1 і P2 відповідають класам К1–К2 і К3–К4 AIS 20 [5].

В AIS 31 перевірка здійснюється на відповідність функціональним класам P1 та P2.

При перевірці на відповідність Р1 використовуються тесті, що були взяті у стандарті FIPS 140-1 [8], але додатково введено автокореляційний тест, що дозволяє перевірити кореляції між послідовністю та зсувом 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.

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 най

Для відповідності ФГВЧ класу Р1 мають виконуватися вимоги Р.1.I-Р1.VI відповідно до механізмів і функцій стійкості [6].

Р.1.I вимагає, щоб послідовність випадкових векторів, утворена із внутрішніх ВЧ r_1, r_2, … із великою ймовірністю була попарно різною (тест Т0).

Для верифікації вимоги Р.1 внутрішні послідовності ВЧ r_1, r_2, … та їхні проекції на окремі біти повинні задовольняти статистичним тестам, що наведені в опису методики AIS 31 [6].

Р.1.III (якщо стійкість механізмів або функцій «середня» або «висока»). Якщо при включенні ФГВЧ відбувається загальне призупинення джерела шуму, то воно має бути негайно ж розпізнане, і після призупинення не можуть бути подані зовнішні випадкові числа.

Р.1.IV (якщо стійкість механізмів або функцій «середня» чи «висока»). Якщо під час роботи ФГВЧ виникає загальне призупинення джерела шуму, то після цього припиняється вироблення випадкових величин, що виробляються внутрішньою випадковою послідовністю. У якості заміни досить, щоб після загального останова джерела шуму ФГВЧ поводився для кожної постійної послідовності сигналів шуму як К2-ДГВЧ AIS 20, вихідні послідовності якого відповідають передбаченій меті застосування.

Р.1.V (якщо стійкість механізмів або функцій «висока»). Необхідні в Р.1.I і Р.1.II властивості мають бути верифіковані при передбачених зовнішніх впливах, оскільки вони можуть впливати на функціонування джерела шуму.

Р.1.VI (якщо стійкість механізмів або функцій «середня» чи «висока»). ФГВЧ повинен містити online-тест, який за зовнішнім запитом перевіряє якість внутрішніх випадкових чисел [6].

Після запуску апаратний генератор шуму починає виробляти плавно керовані блоки неопрацьованих випадкових байтів. Для негайного виявлення несправності фізичного джерела шуму на старті застосовуються повні статистичні випробування (online-тест). Тільки у разі успіху ФГВЧ доходить до стандартного режиму роботи і стає доступним для застосування. У стандартному режимі online-тест застосовується до кожного згенерованого блоку випадкових байтів. Якщо тест пройдений, ФГВЧ повернеться до робочого режиму. Інакше ФГВЧ буде блокований, і, отже, всі запити, що використовують ФГВЧ, будуть повернені з відповідним кодом помилки. Під час роботи кінцевого об'єкта оцінки тестування ФГВЧ має виконуватися безперервно для перевірки правильності його роботи.

Вимоги на відповідність ФГВЧ класу Р2 [6].

ФГВЧ має належати класу Р1 як мінімум з такими самими механізмами та функціями стійкості [6].

Р2.I–Р2.VI Верифікація властивостей Р1.

Р2.VII Дискретизовані послідовності шумових сигналів (ДПШС), що задовольняють певним критеріям, мають проходити статистичні тести, які, крім усього іншого, мають виключити багатокрокові залежності. Крім того, має бути пройдений ентропійний тест [6].

Р2.VIII Додаткова математична обробка не повинна зменшувати ентропію на біт.

Р2.IX (якщо стійкість механізмів або функцій «середня» чи «висока»). При кожному включенні ФГВЧ мають бути засвідчені мінімальні статистичні властивості ДПШС. Доти, поки не закінчиться статистичне тестування, випадкові числа не можуть бути видані.

Р2.X (якщо стійкість механізмів або функцій «середня» або «висока»). Якщо під час роботи ФГВЧ відбулося загальне призупинення джерела шуму, має виключатися видача випадкових чисел, тому що відповідні внутрішні випадкові послідовності були згенеровані після призупиненн.

Р2.XI (якщо стійкість механізмів або функцій «середня» чи «висока»). У роботу ФГВЧ має бути імплементовано online-тест, за допомогою якого може бути перевірена статистична якість дискретизованої послідовності шумового сигналу. Online-тест має бути викликаним ззовні або ж ФГВЧ повинен сам викликати його. Останнє має здійснюватися постійно або принаймні через регулярні проміжки. Online-тест має розпізнати в погоджений час незначні статистичні дефекти або погіршення статистичних властивостей дискретизованої шумової послідовності.

Р2.XII (якщо стійкість механізмів або функцій «висока»). Необхідні в Р2.VII властивості мають бути верифіковані для передбачених зовнішніх умов застосування (t^0, енергопостачання і т.д.), оскільки вони можуть впливати на функціонування джерела шуму.

Р2.XIII (якщо стійкість механізмів або функцій «висока»). ФГВЧ повинен сам викликати online-тест.

В AIS 31 для верифікації зазначених вимог використовуються тести, що наведені в опису методики [6].

Висновки

Основними вимогами, що висуваються до детермінованих генераторів випадкових бітів (ДГВБ), є непередбачуваність, просторова і часова складність, відновлюваність у просторі й часі, необоротність, проходження сформованими послідовностями набору статистичних тестів, а також період повторення.

Запропоновано декілька підходів до визначення рівнів гарантій криптографічної стійкості генераторів випадкових чисел. Перший із них пов'язаний з тестуванням псевдовипадкових бітів на випадковість, для чого, наприклад, застосовується стандарт FIPS 140-1, або AIS 20. Більш детальними є вимоги та механізми реалізації, визначені в AIS 20, що дозволяє реалізувати різні рівні гарантій – К1, К2, К3, К4. При цьому найвищим рівнем гарантій є рівень К4. В AIS 31 визначено два рівні гарантій Р1 і Р2, у яких, по суті, Р1 дещо еквівалентний К1, К2, а Р2 еквівалентний К3, К4. У випадку рівня гарантій К4 вимагається, щоб: псевдовипадкові біти мали статистичні властивості, подібні до статистичних властивостей псевдовипадкових бітів, що генеровані ідеальним ДГВБ; була задана ентропія джерела ключів (тобто наявність ключа генератора є обов'язковою); має бути практично виключена можливість обчислення попередніх і наступних бітів генератора при відомому поточному стані.

Необхідною умовою забезпечення криптографічної стійкості є формування ключів, ключової інформації та певних параметрів на основі використання одночасно як засобів формування фізично випадкових і детермінованих випадкових послідовностей.

Список літератури

1. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. – М.: ИЛ, 1963. – 830 с. (Раздел – Теория связи в секретных системах).

2. Вембо Мао. Современная криптография. Теория и практика. / Вембо Мао. Пер. с англ. – М.: Изд. дом «Вильямс», 2005. – 768 с.

3. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: Монографія / І.Д. Горбенко, Ю.І. Горбенко. – Х.: Видавництво «Форт», 2012. – 880 с.

4. Горбенко І.Д. Теоретичні основи побудови криптографічних систем абсолютної стійкості / І.Д. Горбенко, О.А. Замула // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 4 (111). – С. 101-105.

5. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for Deterministic random number generators. 1999.

6. Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001, 38 pages.

7. ANSI X9. 82, Part 3 – Draft – July 2004. Random Number Generation, Part 3: Deterministic Random Bit Generators.

8. Federal Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994.

9. ISO/IEC FCD 19790: Information technology- Security requirements for cryptographicmodules. Proect: 1.27.40.

10. ISO/IEC 18031 Information technology — Security techniques — Random bit generation. 2005.

11. 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.

Надійшла до редколегії 9.04.2014

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв, Полтавський національний технічний університет ім. Ю. Кондратюка, Полтава.

АНАЛИЗ И ОБОСНОВАНИЕ КРИТЕРИЕВ И ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

А.А. Замула, Д.А. Семченко, Ю.В. Землянко

Приведен анализ требований необходимых при построении систем криптографической защиты информации. Рассмотрены методики оценки статистических свойств псевдослучайных последовательностей. Даны рекомендации по использованию каждой из рассмотренных методик. Указаны необходимые и достаточные условия для создания криптографически стойких генераторов на основании международных и национальных стандартов. Предложены подходы по определению уровней гарантий криптографически стойких генераторов псевдослучайных последовательностей.

Ключевые слова: *генератор, методика, стандарт, уровень гарантий, FIPS PUB 140-1, NIST STS, AIS 20, AIS 31.*

ANALYSIS AND JUSTIFICATION CRITERIA AND MEASURES OF EFFICIENCY CRYPTOGRAPHIC PSEUDO RANDOM NUMBER GENERATORS

A.A. Zamula, D.A. Semchenko, Yu.V. Zemlyanko

Article describes an analysis of the requirements necessary for the construction of cryptographic information security systems. Viewed the evaluation procedures of the statistical properties of pseudorandom sequences. Recommendations on use are given of each of the considered methods. The article presents the necessary and sufficient conditions for creating cryptographically strong generators on the basis of international and national standards. Suggested approaches to determine the levels of safeguards cryptographically strong pseudo-random sequence generator.

Keywords: *generator, methods, standards, level of assurance, FIPS PUB 140-1, NIST STS, AIS 20, AIS 31.*