3. Для повышения точности измерений их необходимо проводить систематизировано с применением специальных приборов, техники и технологий.

4. Анализ величин отклонений размерных признаков типовых фигур позволил обнаружить изменения в типологии женского населения Украины средней возрастной группы. Изменились и линейные, и дуговые показатели. В первую очередь это отразилось в высотах.

5. После обработки результатов антропометрических данных женского населения Украины можно выделить отличительные и схожие закономерности при сравнении с зарубежными данными. Наблюдается общая тенденция населения средней возрастной категории к увеличению дуговых поперечных размеров и изменения пропорциональности показателей высот.

Литература

1. Размерная типология населения с основами анатомии и морфологии / Т.Н.Дунаевская, Е. Б. Коблякова, Г. С. Ивлева, Р. В. Иевлева; Под ред. Е. Б. Кобляковой: Учеб. пособие для студ. учреждений сред. проф. образования. - М.: Мастерство; Издательский центр «Академия», 2001.-288 с.
2. Куршакова Ю. С., Дунаевская Т. Н., Зенкевич П.И. Проблемы размерной антропологической стандартизации для конструирования одежды. М., 1978.
3. Костин Ю.А. Морфологическая характеристика тела человека применительно к проектированию одежды / Учебное пособие: Иваново, ИГТА, 1995.
4. Дунаевская Т. Н., Коблякова Е. Б., Булатова Е.Б. Об осанке тела женщины // Вопросы антропологии.1975.
5. http://www.chniishp.ru.

УДК 681.3.06

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

С.П. Євсеєв
Кандидат технічних наук, доцент
Кафедра інформаційних систем*
Контактний тел.: (057) 702-18-31
E-mail: Evseev_Serg@hneu.edu.ua

Р.В. Корольов
Старший науковий співробітник
Науковий центр
Харківський університет Повітряних Сил ім. І. Кожедуба
вул. Сумська, 77/79, кім. 314, м. Харків, Україна, 61000
Контактний тел.: (057) 700-21-65
E-mail: kljaksa01@ranbler.ru

М.В. Краснянська*
*Харківський національний економічний університет
пр. Леніна, 9а, кім. 412, м. Харків, Україна, 61000
Контактний тел.: 063-227-52-27
E-mail: Mariakrasnyanska@gmail.com

Розглядаються методи формування послідовностей псевдовипадкових чисел, досліджується підхід до побудови доказово безпечних генераторів, стійкість яких обґрунтовується теоретико-складною проблемою синдромного декодування

Ключові слова: послідовності псевдовипадкових чисел, генератор псевдовипадкових чисел

Рассматриваются методы формирования последовательностей псевдослучайных чисел, исследуется подход к построению доказуемо безопасных генераторов, устойчивость которых обосновывается на теоретико-сложностной проблеме синдромного декодирования

Ключевые слова: последовательности псевдослучайных чисел, генератор псевдослучайных чисел

They are considered methods of the shaping the sequences pseudorandom numbes, is researched approach to building provably safe generator, which stability is motivated on theorist-numerical problem decoding of syndrome

Keywords: sequences of pseudorandom numbers, pseudorandom number generator

1. Вступ

В умовах стрімкої інформатизації суспільства, широкого застосування засобів обчислювальної техніки та комп'ютерних систем особливу актуальність набувають питання інформаційної безпеки, найбільш складними з яких є необхідність захисту цінної конфіденційної і секретної інформації в державних і приват-

них підприємствах, в органах і установах державного управління, банківської та інших системах. Збільшення обсягів оброблюваних і переданих даних у комп'ютерних системах та мережах, перш за все в банківських системах вимагає нових підходів до протоколів і механізмам забезпечення безпеки переданих даних [1,2].

2. Постанова проблеми у загальному виді та аналіз літератури

Незважаючи на широке застосування різних криптографічних алгоритмів на різних рівнях захисту інформаційні системи схильні до різних атак і загроз. Під загрозою безпеки інформаційної системи розуміються можливий вплив на інформаційну систему, який прямо чи побічно може завдати шкоди її безпеки.

Для забезпечення захисту від загроз безпеки використовуються різні криптографічні механізми. Для побудови механізмів безпеки інформації традиційно використовують методи криптографічної обробки інформації. Важливе місце у розвитку сучасних механізмів забезпечення безпеки інформаційних систем і технологій займає використання псевдовипадкових випадкових чисел (ПВЧ) і відповідно генераторів псевдовипадкових чисел (ГПВЧ). Вони використовуються для вирішення наступних завдань: хешування інформації; побудови синхронних і самосінхронізуючих поточних шифрів; формування ключової інформації і т.д. [3].

Характеристики систем безпеки в більшості своїй залежать від характеристик їх криптографічних підсистем, які визначаються не тільки алгоритмікою, але й якісними показниками саме використовуваних псевдовипадкових послідовностей. Так як безпека криптосистеми зосереджена на ключі, то при використанні ненадійного процесу генерації ключів, вся криптосистема в цілому так само вразлива [3].

Метою даної статті є аналіз сучасних методів формування псевдовипадкових послідовностей, оцінка переваг та недоліків даних методів та дослідження ГПВЧ заснованих на проблемі декодування випадкового коду Pseudo-Random Generator Provably as Secure as Syndrome Decoding (GPSSD).

3. Оцінка переваг та недоліків сучасних методів формування псевдовипадкових послідовностей

Формування ПВЧ здійснюється за допомогою відповідних ГПВЧ реалізованих на основі відомих методів, які можна розділити на два класи: криптостійкі і некріптостійкі [4]. Класифікація некріптостійких методів наведена на рис. 1.

Широко відомим класом некріптостійких генераторів, є конгруентні генератори [4 – 7]. Найчастіше на практиці використовуються лінійні конгруентні генератори, який має наступна форму [4,7]:

$$x_i = (ax_{i-1} + b) \bmod m \qquad (1)$$

де x_i – і–й елемент псевдовипадкової послідовності; $a \neq 0$ – множник; b – приріст; m – потужність послідовності (модуль).

Період такого генератора не більше, ніж m. Якщо a , b і m вибрано правильно, то генератор буде формувати послідовність з максимальним періодом. Лінійні конгруентні генератори не можна використовувати в криптографії, так як вони передбачувані. Так само ненадійним є квадратичний генератор:

$$x_n = (ax_{n-1}^2 + bx_{n-1} + c) \bmod m \qquad (2)$$

та кубічний генератор:

$$x_n = (ax_{n-1}^3 + bx_{n-1}^2 + cx_{n-1} + d) \bmod m \qquad (3)$$

Основними перевагами конгруентних генераторів є:

– максимальний період сформованої послідовності;

– простота програмної і апаратної реалізації;

– можливість побудови на їх основі генераторів, що мають властивості, необхідні для вирішення прикладних питань захисту інформації.

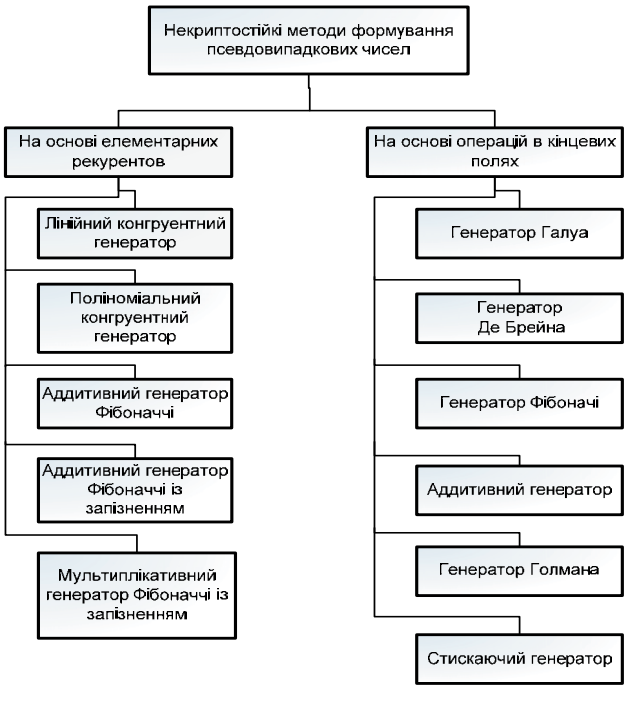

Рис. 1. Некриптостійкі методи формування псевдовипадкових чисел

Основним недоліком таких генераторів є формування псевдовипадкових чисел не криптостійких до різних видів криптоаналізу (кореляційний, інверсний та ін.) Тому конгруентні генератори використовуються для вирішення завдань захисту інформації як складові елементи криптосхем [4, 7]. Наступним прикладом ГПВЧ є регістр зсуву зі зворотним зв'язком. Він складається з двох частин: регістр зсуву і функції зворотного зв'язку. Регістр зсуву являє собою послідовність бітів фіксованої довжини, який наведений на рис. 2.

Функція зворотного зв'язку є булевою функцією з множини L -мірних векторів з координатами з множини (0, 1) в множини (0, 1), L – довжина зсувного регістру. У початковий момент роботи регістр зсуву заповнюється деяким початковим значенням (яке являє собою секретний ключ). На кожному наступному кроці обчислюється значення $y = f(x_0, x_1, \ldots, x_{L-1})$, де x_i –значення клітинки з номером і .

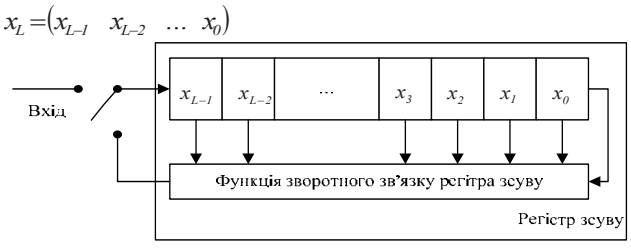

Рис. 2. Регістр зсуву зі зворотним зв'язком

Найпростішим видом регістра зсуву зі зворотним зв'язком є лінійний регістр зсуву зі зворотним зв'язком (linear feedback shift register LFSR). Функція зворотного зв'язку $y = f(x_0, x_1, \dots, x_{L-1})$ є в цьому випадку просто сумою за модулем 2 декількох фіксованих розрядів.

Самі по собі LFSR є хорошими ГПВЧ, але вони мають деякі небажані невипадкові властивості. Послідовні біти лінійні, що робить їх марними для шифрування. Крім того, великі випадкові числа, що генеруються з використанням йдучих підряд бітів цієї послідовності, сильно корельовані і для деяких типів додатків зовсім не є випадковими [7].

Адитивні генератори (запізнюючі генератори Фібоначі) дуже ефективні, оскільки їх результатом є випадкові слова, а не випадкові біти. Самі по собі вони не являються криптографічно стійкими, але їх можна використовувати в якості складових блоків для безпечних генераторів.

Початковий стан генератора являє собою масив n-бітових слів: 8-бітових слів, 16-бітових слів, 32-бітових слів, і т.д.: $x_1, x_2, x_3 \dots x_m$. Цей первісний стан і є ключем. i-те слово генератора виходить як:

$$X_i = (X_{i-p} + X_{i-q}) \bmod m \qquad (4)$$

Якщо многочлен $x^p + x^q + 1$ є примітивним то період такого генератора складе $2^{\log_2 m - 1}(2^q - 1)$.

Прикладами адитивних генераторів є генератори Fish і Pike [9].

Класифікація крипостійких методів наведена на рис. 3.

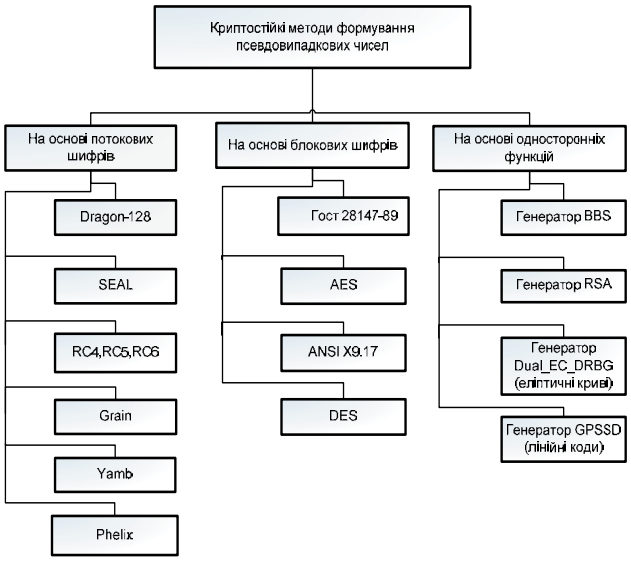

Рис. 3. Криптостійкі методи формування псевдовипадкових чисел

До криптостійких ГПВЧ відносяться генератори, побудовані на основі поточних шифрів. Прикладами можуть служити генератори SEAL, RC4, RC5, RC6, Grain та інші.

Особливістю SEAL є те, що він насправді є не традиційним потоковим шифром, а являє собою сімейство псевдовипадкових функцій. При 160-бітовому ключі k і 32-бітів регістра n, SEAL розтягує n в L-бітовий рядок $k(n)$. L може приймати будь-яке значення, менше 64 Кбайт. SEAL використовує наступне правило: якщо k вибирається випадковим чином, то $k(n)$ має бути не відрізняючим від випадкової L-бітової функції n. Практичний ефект того, що SEAL є сімейством псевдовипадкових функцій, полягає в тому, що він зручний у ряді програм, де не застосовні традиційні потокові шифри. При використанні більшості поточних шифрів створюється односпрямована послідовність біт: єдиним способом визначити i-й біт (знаючи ключ і позицію i) є генерування всіх бітів аж до i-го. Відмінність сімейства псевдовипадкових функцій полягає в тому, що можна легко отримати доступ до будь-якої позиції ключової послідовності.

Особливістю SEAL є те, що він насправді є не традиційним потоковим шифром, а являє собою сімейство псевдовипадкових функцій. При 160-бітовому ключі k і 32-бітів регістра n, SEAL розтягує n в L-бітовий рядок $k(n)$. L може приймати будь-яке значення, менше 64 Кбайт. SEAL використовує наступне правило: якщо k вибирається випадковим чином, то $k(n)$ має бути не відрізняючим від випадкової L-бітової функції n. Практичний ефект того, що SEAL є сімейством псевдовипадкових функцій, полягає в тому, що він зручний у ряді програм, де не застосовні традиційні потокові шифри. При використанні більшості поточних шифрів створюється односпрямована послідовність біт: єдиним способом визначити i-й біт (знаючи ключ і позицію i) є генерування всіх бітів аж до i-го. Відмінність сімейства псевдовипадкових функцій полягає в тому, що можна легко отримати доступ до будь-якої позиції ключової послідовності.

Основною перевагою ГПВЧ побудованих на основі поточних шифрів є висока швидкість перетворення, порівнянна зі швидкістю надходження вхідної інформації. Таким чином, забезпечується формування ПВЧ в реальному масштабі часу [15].

До недоліків можна віднести необхідність синхронізації на приймальній та передаючій сторонах [4, 7].

Наступним класом криптостійких генераторів є ГПВЧ побудовані на блочних шифрах [7-9]. Робота таких генераторів полягає в застосуванні до блоку відкритого тексту багаторазового математичного перетворення. Багатократність застосування обумовлює те, що результуюче перетворення виявляється криптографічно більш складним, ніж саме перетворення. Основна мета здійснюваних перетворень – це створити залежність кожного біта блоку зашифрованого повідомлення від кожного біта ключа і кожного біта блоку відкритого повідомлення. Перетворення, що лежать в основі даних алгоритмів можна розділити на «складні» перетворення, в сучасних алгоритмах це зазвичай нелінійні операції, і «прості» перетворення, в

основі яких лежать перемішуючі операції. Аналітична складність розкриття алгоритмів блокового шифрування лежить в основному на конструкції першого типу перетворень.

Основною перевагою ГПВЧ побудованих на основі блокових шифрів є: хороші статистичні властивості формованої псевдовипадковою послідовності і стійкість до різних видів криптоаналізу (кореляційний, інверсний та ін.) [7 – 9].

До основних недоліків блокового шифрування можна віднести:

– нечутливість кріптосхем до випадання або вставці цілого числа блоків;

– існування проблеми останнього блоку неповної довжини.

Особливим напрямком у розвитку криптостійких генераторів одержали методи, що допускають застосовність моделі доказовою стійкості. До них належать методи, засновані на вирішенні односторонніх функцій [7, 12].

Функція $F:\{0,1\}^n \to \{0,1\}^m$ називається односторонньою функцією, якщо:

– функція F обчислювана за поліноміальний час;

– не існує поліноміального алгоритму, який вірно обчислює $F-1$ з гарною ймовірністю;

– існує предикат $h:\{0,1\}^n \to \{0,1\}$, т.щ. по $F(x)$ важко обчислити $h(x)$.

В даний час теорія алгоритмів не дозволяє довести не існування ефективних алгоритмів вирішення того чи іншого завдання.

Не будь-яка одностороння функція не може бути використана для шифрування. Для використання в криптографії необхідно, щоб завдання інвертування шифрувального перетворення (тобто обчислення t по $F(t)$) була розв'язана за прийнятний час, але зробити це міг тільки той, хто знає секретний ключ. Такі функції називаються односторонніми функціями з секретом (або з потайним ходом). Для практичних цілей криптографії було побудовано декілька функцій, які можуть виявитися функціями з секретом. Найбільш відомою і популярною з них є теоретико-числена функція, на якій побудований шифр RSA [7].

Генератори, засновані на вирішенні односторонніх функцій, називаються доказово стійкими генераторами. До доказово стійких генераторів відносяться ГПВЧ BBS і RSA.

Генератор BBS (Blum-Blum-Shub), стійкість якого ґрунтується на теоретико- складносної задачі обчислення примітивних квадратних коренів за модулем числа Блюма, еквівалентної з обчислювальною складністю задачі факторизації (розкладання числа на співмножники).

Істотним недоліком таких генераторів є висока обчислювальна складність, яка визначається, перш за все, великою розрядністю чисел, над якими необхідно виконувати математичні операції, що істотно знижує швидкість формування ПВЧ в порівнянні з генераторами, заснованими на блочних або поточних шифрах [7,10-12].

Виняток становлять доказово-стійкі ГПВЧ, обчислення секретного ключа в яких зводиться до розв'язання теоретико-складностної задачі синдромного декодування [10]. У цьому випадку складність формування ПВЧ визначається процедурами кодування лінійних надмірних кодів, що зіставно по швидкодії з симетричним криптографічним перетворенням.

4. Аналіз ГПВЧ заснованих на проблемі декодування випадкового коду.

Доказово стійкий генератор ПВЧ на надмірних кодах GPSSD вперше запропонований в [12]. Основна ідея такого генератора полягає у використанні алгебраїчного блокового коду з легко реалізованими алгоритмами кодування та декодування [10-12]. За допомогою маскування алгебраїчного коду під випадковий код, завдання декодування для зловмисника представляється як обчислювально складна.

В ході проведених досліджень був проведений аналіз статистичних властивостей добре відомих ГПСЧ і генератора GPPSD . Результати досліджень представлені в табл.. 1. Отримані результати показали, що найбільші показники статистичної безпеки показали такі ГПСЧ як: лінійний конгруентний генератор, BBS, G using DES, GPSSD. Як випливає з табл. 1. ГПСЧ GPPSD не поступається по своїх статистичних властивостях відомим ГПСЧ.

Для оцінки періоду сформованої ПВП генератором GPPSD, була розроблена його програмна реалізація, як початкові дані використовувався лінійний блоковий код (64,24,16) . В ході дослідження проаналізовані всі ключові дані і проведена оцінка довжини періодів ПВЧ. Очікуваний період формованої послідовності повинен був скласти $2^{24}-1$ біт, але насправді він виявився на 5 порядків нижче максимального що потенційно може привести до появи криптографічних атак.

Таблица 1

Результати експериментальних досліджень відомих ГПСЧ

ГПВЧ	Кількість тестів, в яких тестування пройшло М послідовностей (%)		
	M ≥ 99%	M ≥ 96%	M < 96%
G using SHA-1	122(65%)	188 (99,5%)	1 (0,5%)
Linear Congruential	139 (74%)	189 (100%)	–
Micali-Schnorr	130 (69%)	189 (100%)	–
Quadratic Congruential	124 (66%)	181 (96%)	8 (4%)
G using DES	142 (75%)	188 (99,5%)	1 (0,5%)
ANSI X9.17 (3-DES)	121 (64%)	187 (98%)	4 (2%)
Blum-Blum-Shub	134 (71%)	189 (100%)	–
FIPS 197	126 (67%)	189 (100%)	–
GPSSD для коду (1024,453,128)	140 (76%)	189 (100%)	–

Проведені дослідження ефективності генератора на надлишкових кодах (GPSSD), показали, що поряд з високими показниками статистичної безпеки і ви-

сокою швидкістю формування, даний генератор має один істотний недолік: період сформованої послідовності не є максимальним, що не задовольняє одній з основних вимог до кріптогрфічно стійкого генератора [10]. У роботі [11] розглянуто удосконалений метод формування ПВЧ. Основною перевагою вдосконаленого методу перед методом-прототипом GPSSD є забезпечення максимального періоду формуються ПВЧ. За своєю структурою запропонований метод передбачає виконання простих і ефективних обчислювально операцій які дозволяють формувати ПВЧ у реальному масштабі часу.

5. Висновки

Проведенні дослідження показали, що існуючі методи формування псевдовипадкових послідовностей мають ряд недоліків та не задовольняють потреб сучасної криптографії. Розглянутий удосконалений метод формування ПВЧ GPSSD має високі показники статистичної безпеки і високу швидкість та максимальний період формування псевдовипадкових послідовностей.

Перспективним напрямом подальших досліджень є розробка метода швидкого формуваня ПВЧ зі зведенням завдачі криптоаналіза до рішення теоретико-складностного завдання декодування випадкового коду по відомому кодовому слову з помилками як функції від секретного вектора-ключа.

Література

1. Задірака В.К. Методи захисту банківської інформації. / В.К. Задірака, О.С. Олесюк, Н.О. Недашковський - Київ. Вища школа, 1999 – 264 с.
2. Конеев И. Р. Информационная безопасность предприятия / И. Р.Конеев, А.В. Беляев - Спб.: БХВ-Петербург, 2003. – 752 с.
3. Інформаційний портал Все об IT [Електронний ресурс] Режим доступу до журн. : http://itc.ua.
4. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайной последовательности – Мjсква. «Кудиц-Образ». 2003 – 240с.
5. Интернет Университет Информационных Технологий [Електронний ресурс] Режим доступу до журн. : http://www.intuit.ru/.
6. Столингс В. Криптография и защита сетей: принципы и практика, 2-е изд. : пер. с англ. — М.: издательский дом «Вильям», 2001. — 672 с.
7. Шнайер Б. Практическая криптография / Шнайер Б., Фергюсон Н. – Издательский дом «Вильямс». 2005. – 423с.
8. Брассар Ж. Современная криптография – Поли мед. 1999. - 178с.
9. Кузнецов А.А. Исследование статистической безопасности генераторов псевдослучайных чисел / А.А. Кузнецов, Р.В. Королев, Ю.Н. Рябуха // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип. 3 (70). – С. 79-82.
10. Кузнецов А.А. Усовершенствованный метод быстрого формирования последовательностей псевдослучайных чисел/ Зб. наук. пр. "Кібернетика та системний аналіз"/ Кузнецов А.А., Королёв Р.В., Рябуха Ю.Н./ ХНВС. - Харьков:2008.
11. Кузнецов О. О. Метод швидкого формування послідовностей псевдовипадкових чисел доказової стійкості/ Зб. наук. пр. "Теоретичні основи розробки систем озброєння"/ Кузнецов А.А., Королёв Р.В., Рябуха Ю.Н./ ХНВС. - Харьков:2008.
12. J. Fisher. An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding / Jean-Dernard Fisher, Stern Jacques // EUROCRYPT'96 Proceeding, LNCS 1070. – P. 245 – 255. 6.