7. Llerena L. et al. Applying a Usability Technique in the LibreOffice Writer Project // CLEI ELECTRONIC JOURNAL. – 2020. – Т. 23. – № 2.

Ключові слова: відкрите програмне забезпечення, відкриті формати даних, відкриті протоколи взаємодії, загрози і ризики, освіта.
Ключевые слова: открытое программное обеспечение, открытые форматы данных, открытые протоколы взаимодействия, угрозы и риски, образование.
Key words: open software, open data formats, open communication protocols, threats and risks, education.

СОКОЛОВ АРТЕМ ВИКТОРОВИЧ

Национальный университет «Одесская юридическая академия»,
доцент кафедры кибербезопасности,
кандидат технических наук, доцент

ХИМЕНКО МИХАИЛ ВАЛЕРЬЕВИЧ

Государственный университет «Одесская политехника»,
студент бакалавриата

ТЕСТИРОВАНИЕ ГЕНЕРАТОРОВ КЛЮЧЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ СОВЕРШЕННЫХ АЛГЕБРАИЧЕСКИХ КОНСТРУКЦИЙ

Одной из важнейших составных частей современных систем защиты информации являются криптографически стойкие генераторы псевдослучайных ключевых последовательностей (ГПКП). Важным свойством современных ГПКП является их способность вырабатывать псевдослучайные последовательности G большой длины $|G|$ на основе криптографического ключа K незначительной длины $|G|$, т. е. $|G| \gg |K|$. При этом, с одной стороны результирующая последовательность должна обладать значительным уровнем стохастического качества, тогда как с другой стороны её восстановление должно быть возможно только в случае наличия криптографического ключа K.

ГПКП нашли свои значительные применения в системах защиты информации, основанных на концепции оперативной смены ключа [1], для генерации векторов инициализации, являются основным элементом современных поточных шифров, обеспечивающим выработку гаммы, которая впоследствии накладывается на шифруемую информацию.

В настоящее время предложены также схемы ускорения шифрования информации блочными симметричными шифрами [2], основанные на использовании ГПКП. При этом качество шифрования информации будет напрямую зависеть от качества используемой гаммы.

Другой важнейшей характеристикой ГПКП, на которою опираются при выборе конкретной схемы данного криптографического примитива, является их быстродействие.

В последнее время значительное распространение получили ГПКП на основе совершенных алгебраических конструкций – бент-последовательностей [3] за счет высокого качества генерируемых ими псевдослучайных последовательностей и достаточно высокой скорости их работы.

Одной из перспективных разработок является ГПКП на основе совершенных алгебраических конструкций (бент-последовательностей и последовательностей де Брейна), а также математического аппарата клеточных автоматов, который используется вместо Регистров Сдвига с Линейной Обратной Связью (РСЛОС), как это сделано в работе [3].

В работах [3] и [4] проведено тестирование разработанных генераторов с помощью набора стохастических тестов Иванова-Чугункова [5], тем не менее в настоящее время тестирование стохастического качества любой последовательности, в частности, генерируемой с помощью ГПКП, выполняется с помощью более строгого набора стохастических тестов NIST [6].

Данный набор включает 15 стохастических тестов, которые считаются пройденными если их результат превышает значение 0.01. Тесты NIST позволяют выявить даже незначительные закономерности, которые могут оставаться незамеченными при использовании набора тестов [5], который применялся в работах [3] и [4].

В настоящей работе с помощью пакета стохастических тестов NIST мы представляем сравнительную характеристику генераторов на основе совершенных алгебраических конструкций и РСЛОС [3] и на основе совершенных алгебраических конструкций и клеточных автоматов [4].

Для эксперимента с помощью обеих ГПКП [3] и [4] были сгенерированы файлы длиной 400 Кб, что является достаточным для проведения каждого из тестов. После генерации к полученным файлам был применен набор стохастических тестов NIST.

Результаты тестирования представлены в табл. 1.

Анализ данных, представленных в табл. 1 свидетельствует о том, что последовательности, сгенерированные с помощью ГПКП на основе клеточных автоматов, будучи соответствующими тестам Иванова-Чугункова, не соответствуют большинству тестов NIST, за исключением тестов Non overlapping template matching, Random excursion, Random excursion variant. В случае использовании ГПКП на основе РСЛОС большинство тестов, за исключением теста DFT, выполняется.

Указанное актуализирует задачу дальнейшего совершенствования структуры ГПКП на основе совершенных алгебраических конструкций, для улучшения их криптографического качества до уровня соответствия современному набору тестов NIST, что станет предметом дальнейших исследований.

Таблица 1

Результаты тестирования ГПКП

№	Тест	Генератор на основе клеточных автоматов [4]		Генератор на основе РСЛОС [3]	
		P-value	Pass rate	P-value	Pass rate
1	Monobit test	$1.92 \cdot 10^{-85}$	✘	0.48	✔
2	Frequency within block test	$1.31 \cdot 10^{-36}$	✘	0.7	✔
3	Runs test	0	✘	0.2	✔
4	Longest run ones in a block test	$1.08 \cdot 10^{-40}$	✘	0.02	✔
5	Binary matrix rank test	0	✘	0.76	✔
6	DFT test	0	✘	0	✘
7	Non overlapping template matching test	1	✔	1	✔
8	Overlapping template matching test	$1.94 \cdot 10^{-19}$	✘	0.38	✔
9	Maurers universal test	$3.5 \cdot 10^{-17}$	✘	0.84	✔
10	Linear complexity test	$1.53 \cdot 10^{-23}$	✘	0.14	✔
11	Serial test	$3.11 \cdot 10^{-240}$	✘	0.45	✔
12	Approximate entropy test	$3.54 \cdot 10^{-240}$	✘	0.65	✔
13	Cumulative sums test	0	✘	0.45	✔
14	Random excursion test	0.16	✔	0.05	✔
15	Random excursion variant test	0.09	✔	0.03	✔

Список использованной литературы:

1. Мазурков М. И. Системы широкополосной радиосвязи. Одесса : Наука и Техника, 2010. С. 340.
2. Соколов А. В., Корж А. О. Исследование режимов шифрования с пропуском блоков. Информатика и математические методы в моделировании. 2020. Т. 10, № 1/2. С. 100–108.
3. Мазурков М. И., Соколов А. В., Барабанов Н. А. Генератор ключевых последовательностей на основе дуальных пар бент-функций. Праці Одеського політехнічного університету. 2013. № 3. С. 150–156.
4. Соколов А. В. Быстродействующий генератор ключевых последовательностей на основе клеточных автоматов. Праці Одеського політехнічного університету. 2014. № 1 (43). С. 180–186.
5. Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М. : КУДИЦ-ОБРАЗ, 2003. 240 с.

6. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal et al. National Institute of Standards and Technology Special Publication, 2010. 131 p.

Ключові слова: криптографія, генератор псевдовипадкових ключових послідовностей, стохастичний тест.
Ключевые слова: криптография, генератор псевдослучайных ключевых последовательностей, стохастический тест.
Key words: cryptography, pseudo-random key sequence generator, stochastic test.

КУХАРЕНКО СЕРГІЙ ВІКТОРОВИЧ

Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат технічних наук

ПІДХІД ЩОДО ОБҐРУНТУВАННЯ ВИМОГ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Впровадження сучасних цифрових технологій в різні сфери життя і виробництва та комп'ютеризація повсякденного життя, електронний документообіг, створення великих баз даних, необхідність прийняття відповідальних рішень за короткий час або в критичних ситуаціях, необхідність обробки великих об'ємів інформації тощо потребує створення у кожній без виключення державній установі, комерційних структурах, автоматизованих інформаційно-аналітичних систем управління. Це потребує створення системи захисту інформації та її об'єднання з автоматизованою системою управління (АСУ) в єдину систему та встановлення жорстких логічних та функціональних зв'язків між ними. Як показує практика, саме якість зазначених зв'язків визначає рівень ефективності автоматизованої системи управління з системою безпеки інформації.

Згідно ДСТУ 3396.0/1-96 «ТЗІ. Основні положення (п. 3.2) можливі такі варіанти організації захисту інформації:

- досягнення необхідного рівня захисту за мінімальних затрат і допустимого рівня обмежень видів інформаційної діяльності;
- досягнення необхідного рівня захисту за допустимих затрат і заданого рівня обмежень видів інформаційної діяльності;
- досягнення максимального рівня захисту за необхідних затрат і мінімального рівня обмежень видів інформаційної діяльності.

Відомі методичні рекомендації щодо захисту інформації в АСУ орієнтовані в першу чергу на розроблювачів інформаційних систем, а не на користувачів чи системних адміністраторів або менеджерів безпеки. Водночас з практичної точки зору більш важливі рекомендації, які дають не строго оптимальне, а досить ефективне рішення щодо захисту інформації.