МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ВОЛОДИМИРА ДАЛЯ

ІНФОРМАЦІЙНА БЕЗПЕКА

Науковий журнал

№3 (31) 2018

№4 (32) 2018

Северодонецьк 2018

Інформаційна безпека

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

№3 (31) 2018

№4 (32) 2018

НАУКОВИЙ ЖУРНАЛ

ЗАСНОВАНО У 2009 РОЦІ

ВИХІД З ДРУКУ – ЧОТИРИ РАЗИ НА РІК

ЗАСНОВНИК

Східноукраїнський національний університет ім. Володимира Даля

Журнал зареєстровано Міністерством юстиції України

Свідоцтво про державну реєстрацію **серія КВ №15063-3635Р**

Information security

VOLODYMYR DAHL EAST UKRAINIAN NATIONAL UNIVERSITY

№3 (31) 2018

№4 (32) 2018

THE FIRST ISSUE OF THE JOURNAL WAS PUBLISHED IN 2009

THE JOURNAL IS PUBLISHED QUARTERLY

FOUNDER

Volodymyr Dahl East Ukrainian National University

REGISTERED by the Ministery of Justice of Ukraine registration **sertificate KB №15063-3635P**

ISSN 2224-9613

Відповідальний за випуск: проф., д.т.н. О.С. Петров.

До журналу увійшли статті студентів, аспірантів, докторантів Східноукраїнського національного університету імені Володимира Даля, вищих навчальних закладів України, Росії та закордонних країн.
Журнал підготовлено кафедрою безпеки інформаційних систем СНУ ім. В. Даля.
Рекомендовано до друку Вченою радою Східноукраїнського національного університету імені Володимира Даля (протокол №2 від 26.09.2018 р.).
Занесений до "Переліку фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук" ***з технічних наук***, затверджений постановою президії ВАК України від 14.05.2010 р., №1-05/3.
Матеріали номера друкуються мовою оригіналу.

ЗМІСТ ЖУРНАЛУ №4 (32) 2018

Баранов Г.Л., Міронова В.Л.	ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПРОГНОЗУВАННЯ ТА ГАРАНТУВАННЯ ПОКАЗНИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОГРАМНО-АПАРАТНИХ КОМПЛЕКСІВ	**99**
Грищук Р.В., Скачек Л.Н., Хорошко В.А. Шелест М.Е.	ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО: КОНФЛИКТЫ И ПРОТИВОСТОНИЕ	**106**
Евсеев С.П., Королев Р.В., Белоус Д.М.	РЕЗУЛЬТАТЫ ОЦЕНКИ ПЕРИОДИЧЕСКИХ СВОЙСТВ S-BOX АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ RC4	**116**
Хорошко В.А., Хохлачева Ю.Е.	ПОКАЗАТЕЛИ ДЛЯ ОЦЕНКИ ЖИВУЧЕСТИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА	**123**
Молодецька К.В.	СИСТЕМА НЕЧІТКОГО ВИВЕДЕННЯ ДЛЯ ВИБОРУ МОДЕЛІ СИНЕРГЕТИЧНОГО УПРАВЛІННЯ ВЗАЄМОДІЄЮ АКТОРІВ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ	**129**
Бобок И.И., Кобозева А.А.	ИССЛЕДОВАНИЕ СВОЙСТВ СИНГУЛЯРНЫХ ЧИСЕЛ МАТРИЦ ОРИГИНАЛЬНЫХ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ, ХРАНИМЫХ В ФОРМАТАХ С ПОТЕРЯМИ И БЕЗ ПОТЕРЬ	**134**
Іванченко Є.В., Іванченко І.С., Казмірчук С.В., Шаховал О.А.	ФОРМУВАННЯ МОДЕЛІ КОНТЕКСТНОЇ ЗАЛЕЖНОСТІ ЕЛЕМЕНТІВ ІНФОРМАЦІЙНИХ РЕСУРСІВ	**145**
Опірський І.Р., Сусукайло В.А., Василишин С.І., Луковський Т.І.	РОЗРОБКА МЕТОДУ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ NFC ДЛЯ АВТОМАТИЗОВАНОЇ РЕПЛІКАЦІЇ ПРОФІЛЮ КОРИСТУВАЧА	**151**
Кононова І.В., Креденцер Б.П., Могилевич Д.І.	УРАХУВАННЯ ЗБОЇВ ПРИ ОЦІНЦІ НАДІЙНОСТІ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ З ЧАСОВИМ РЕЗУЛЬТАТОМ	**157**
Хусаінов П.В., Кузавков В.В.	ВЛАСТИВОСТІ СКЛАДНИХ СТРУКТУР ФІЗИЧНИХ, ІНФОРМАЦІЙНИХ ЗВ’ЯЗКІВ БАГАТОЕЛЕМЕНТНИХ ПРОГРАМНО-АПАРАТНИХ ОБ’ЄКТІВ	**166**
Редзюк Є.В.	ЗАСТОСУВАННЯ ВДОСКОНАЛЕНОГО ІНДУКЦІЙНОГО МЕТОДУ	**172**
Бовда Е.М.	МЕТОДИКА Й АЛГОРИТМ ГОРИЗОНТАЛЬНОЇ СТРУКТУРИЗАЦІЇ ЗАДАЧ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ	**178**
Бриль В.М.	ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРВЛІННЯ ПІДПРИЄМСТВОМ НА ОСНОВІ МЕХАНІЗМУ РЕІНЖЕНІРИНГУ БІЗНЕС-ПРОЦЕСІВ	**188**
Артемов В.Ю., Литвиненко Н.І.	ПРОФЕСІЙНА КОМПЕТЕНТНІСТЬ ФАХІВЦІВ, ЯКІ ПРАЦЮЮТЬ У СФЕРІ ІТ-ТЕХНОЛОГІЙ: ДЕОНТОЛОГІЧНИЙ АСПЕКТ	**194**

УДК 681.3.06

[1]Евсеев С.П., [2]Королев Р.В., [2]Белоус Д.М.

[1]Харьковский национальный экономический университет им. С. Кузнеца
[2]Харьковский университет Воздушных Сил им. Ивана Кожедуба

РЕЗУЛЬТАТЫ ОЦЕНКИ ПЕРИОДИЧЕСКИХ СВОЙСТВ S-BOX АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ RC4

В работе проведены исследования периодичных свойств последовательностей псевдослучайных чисел, формируемых генератором RC4. Проведенные исследования формирования S-box для алгоритма шифрования RC-4 показали, что рассмотренный генератор обладает “слабыми” ключами, использование которых приводит к формированию последовательностей псевдослучайных чисел с малым периодом, что в свою очередь может привести к успешным криптографическим атакам.

Ключевые слова: генератор псевдослучайных чисел, поточный шифр, криптографические атаки, мини-версия криптоалгоритма.

Постановка проблемы в общем виде и ее связь с важными практическими заданиями. Алгоритм поточного шифрования RC4 разработан в 1987 г. Рональдом Линном Риверстом, известным американским специалистом в области криптографии для компании RSA DataSecurity [1,2,3]. В течении семи лет этот алгоритм был фирменным секретом и детали о его конструкции предоставлялось только после подписания договора о не разглашении, но в 1994 г. был анонимно опубликован [2]. Начиная с этого времени, он нашел широкое применение в целом ряде криптографических приложений, включая такие, как SSL и TLS – для шифрования данных, передаваемых по сетям ЭВМ, не предусматривающим защиты пользовательских данных, WPA и WEP-для защиты беспроводных соединений [4]. Таким широким распространением алгоритм обязан ряду свойств, не утратившим актуальности за двадцать лет с его существования. Одно из них – высокое быстродействие. Развитие высоких технологий требует от вычислительной техники существенного увеличения быстродействия при использовании ресурсоемких методов шифрования для возросших объемов обрабатываемых данных, что до известной степени нивелирует указанное преимущество. Помимо этого, появилось множество мобильных устройств, для которых главной характеристикой является низкое энергопотребление, а, следовательно, к ним предъявляются требования к снижению энергозатрат используемых алгоритмов на вычислительные операции, что позволяет существенно расширить спектр их применения на различных программно-аппаратных устройствах и платформах.

Анализ последних исследований [4 – 22] показал, что при построении защиты информации в протоколах Интернет технологий на основе блочных и поточных криптоалгоритмов особое значение имеет использование в алгоритмах “сильных” ключевых последовательностей для обеспечения требуемых показателей криптостойкости и быстродействия криптопреобразований.

В работе [4] приведены результаты исследований ключевых пространств и соответствующих им длин периодов формируемых псевдослучайных последовательностей, частично выявлены “слабые” ключи, которые могут привести к компрометации ключевых данных и взлому криптоалгоритма в целом. Однако, проведенные исследования носят ограниченный характер и являются не полными. **Целью статьи** является исследование периодических свойств S-box алгоритма и выявление всех “слабых” ключей на основе методики использования мини-версии генератора RC4, обобщении полученных результатов для полной версии алгоритма.

Изложение основного материала.

Структура и особенности реализации генератора ПСЧ RC4.

Описание алгоритма поточного шифрования RC4 наиболее полно представлено в [1–3]. Алгоритм функционирует независимо от открытого текста, формируемая им

последовательность накладывается на открытый текст, тем самым можно утверждать, что в сущности, алгоритм RC4 является генератором псевдослучайных чисел (ГПСЧ). RC4 содержит подстановочную таблицу (S-бокс): $S_0, S_1, ...S_{255}$ где $S_k \in GF(2^n)$ $n = 8$, $k \in 0 \div 255$ и представляет собой перестановку от 0 до 255. Внутреннее состояние алгоритма, оперирующего элементами из *n* бит, определяется двумя индексными элементами *i* и *j* такой же длины (при начальной инициализации $i, j = 0$).

Для генерации псевдослучайного бита последовательности выполняются следующие операции:

$i = (i + 1) \bmod 256$

$j = (j + S_i) \bmod 256$

$S_i \leftrightarrow S_j$

$t = (S_i + S_j) \bmod 256$

$gamma = S_t$

Значение *gamma* складывается операцией $\oplus$ (сложение по $\bmod 2$) с открытым текстом для формирования шифротекста, либо операции $\oplus$ с шифртекстом для получения открытого текста. Шифрование происходит весьма быстро – примерно в 10 раз быстрее шифра DES [1]. RC4 формирует псевдослучайные последовательности с длинной периода $< 2^{1700} = (256! \times 256^2)$ (возможные состояния шифра). S-бокс медленно изменяется в процессе работы: параметр *i* обеспечивает изменение каждого элемента, а *j* отвечает за то, чтобы эти элементы изменялись псевдослучайным образом.

Методика исследований и основные полученные результаты.

Методика исследования периодических свойств генератора псевдослучайных чисел RC4 над его мини-версией предложена в статье [4], она состоит в построении уменьшенной версии алгоритма RC4 которая, получается, посредством масштабирования с сохранением всех базовых операций алгоритма. Такой подход предложен учеными кафедры безопасности информационных технологий ХНУРЕ при исследовании криптографических свойств БСШ [6–9]. Мини-версия подвергается тестированию и эмпирической оценки длин периодов на различных входных ключевых данных.

Для проведения исследований периодических свойств ГПСЧ RC4 разработаны программные реализации мини-версий над $GF(2^2)$, $GF(2^3)$, т.е используются S-боксы $S_0^1, S_1^1, ...S_3^1$ и $S_0^2, S_1^2, ...S_7^2$ соответственно. Ожидаемые длины периодов должны были составлять $L^1 < 4! * 4^2 = 384$ и $L^2 < 8! * 8^2 = 2580480$ возможных состояний.

Для проведения исследований протестирована работа ГПСЧ RC4 на полном множестве ненулевых ключевых данных и при начальной инициализации $i, j = 0$ (всего 4! ключей для поля $GF(2^2)$ и 8! ключей для поля $GF(2^3)$). В каждом тесте оценивалась длина периода *L*.

В результате проведения эксперимента подсчитаны распределения числа периодов и их количество, которые представлены на рис.1, 2.

Как следует из приведенных на рис. 1, 2 данных, генератор RC4 формирует последовательности с длинного периода ниже максимального. Особый интерес представляют результаты исследования периодических свойств мини-версии RC4 для поля $GF(2^3)$. Существуют “аномально” плохие начальные состояния S-бокса, которые порождают псевдослучайные последовательности с длинной периода на несколько порядков ниже максимально допустимого.

Например, начальные перестановки:

$S_0 = 3, S_1 = 5, S_2 = 6, S_3 = 2, S_4 = 7, S_5 = 0, S_6 = 4, S_7 = 1$

$S_0 = 5, S_1 = 4, S_2 = 1, S_3 = 7, S_4 = 6, S_5 = 2, S_6 = 0, S_7 = 3$

формируют псевдослучайные последовательности с длиною периода 24 элемента, а перестановки:

$S_0 = 5, S_1 = 3, S_2 = 6, S_3 = 4, S_4 = 0, S_5 = 7, S_6 = 1, S_7 = 2$,

$S_0 = 5, S_1 = 3, S_2 = 6, S_3 = 4, S_4 = 1, S_5 = 7, S_6 = 0, S_7 = 2$, $S_0 = 6, S_1 = 4, S_2 = 3, S_3 = 2, S_4 = 7, S_5 = 0, S_6 = 5, S_7 = 1$

$S_0 = 6, S_1 = 4, S_2 = 3, S_3 = 2, S_4 = 7, S_5 = 1, S_6 = 5, S_7 = 0$

формируют псевдослучайные последовательности с длиною периода 120 элемента.

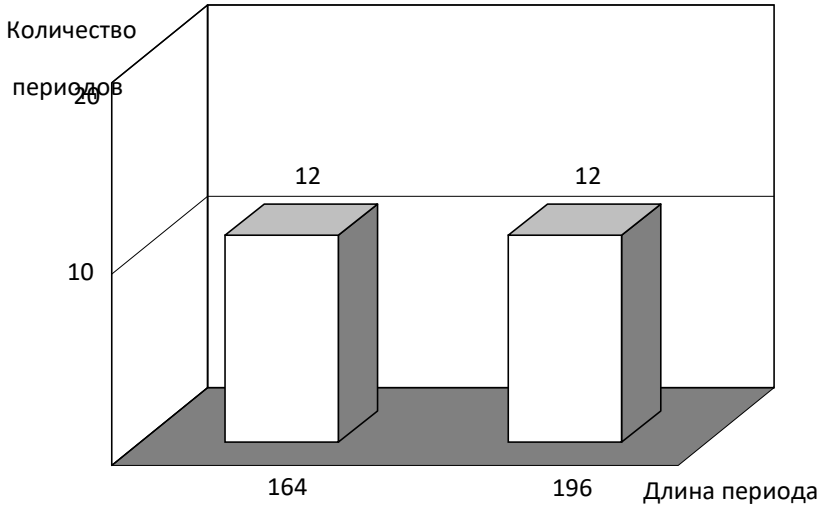

Рис.1. Распределения числа периодов мини-версии RC4 для $GF(2^2)$

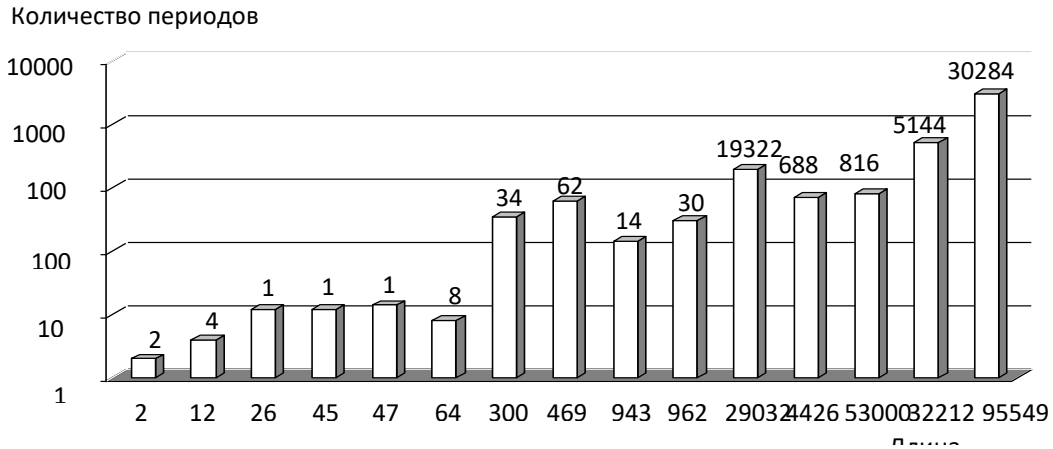

Рис.2. Распределения числа периодов мини-версии RC4 для поля $GF(2^3)$

Кроме того, исследование периодических свойств мини версий показала, что существует зависимость расположения в S-боксе ($S_0, S_1, ...S_n$) единичного значения и начальными значениями i, j которое приводит к формированию ПСП малого периода.

Для проведения исследований протестирована работа ГПСЧ RC4 для поля $GF(2^4)$ на полном множестве ненулевых ключевых данных и при начальной инициализации $i, j = 0$ (всего 16! ключей). Вычислялись значения i, j при которых длинна периода была минимальной.

В ходе проведенных исследований было установлено, что при любом значении S- бокса существует значение i, j при которых длина периода составляет 240 элементов псевдослучайной последовательности. В таблице 1 частично представлены результаты проведенного эксперимента.

Таблица 1

Значения *S*-бокса алгоритма RC4

Значение S-бокса																*i*	*j*	Длина периода ПСП
S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}			
3	6	5	2	4	7	10	**1**	11	12	15	14	8	9	0	13	6	7	240
4	9	5	2	3	12	10	8	11	7	15	13	**1**	6	0	14	11	12	240
15	13	11	9	7	5	3	0	**1**	2	4	6	8	10	12	14	7	8	240
8	13	12	14	7	**1**	3	6	2	5	4	0	15	10	11	9	4	5	240
1	2	4	6	7	3	5	8	10	11	12	13	0	14	9	15	15	0	240
1	15	3	5	7	4	2	0	6	14	13	12	11	10	9	8	15	0	240
1	10	9	5	7	15	6	0	2	14	13	11	12	3	4	**1**	14	15	240

Как следует из приведенных в таблице 1 данных существует зависимость расположения единичного элемента в S-боксе и значениями i, j при которых формируется псевдопоследовательность с малым периодом. Значение j всегда совпадает с номером расположения единичного элемента в S-боксе, а $i = j - 1$ (только для случая когда единичный элемент расположен в диапазоне $S_1 \div S_{15}$). Для случая когда $S_0 = 1$ значение i равно номеру последнего элемента S-бокса, а. $j = 0$. Для проверки выдвинутого предположения протестирована работа ГПСЧ RC4 для поля $GF(2^5)$ и $GF(2^6)$. Длина периода при предложенных значениях i, j составила 992 и 4032 элемента последовательности соответственно, что подтверждает выдвинутое предположение.

Кроме того, в ходе проведенных экспериментов выявлены частные результаты, полученные ранее другими авторами в работе [4], что согласует и дополняет известные положения. Таким образом можно утверждать, что существуют значения секретного ключа (значения S-бокса) при которых формируемые псевдослучайные последовательности имеют период на несколько порядков меньше максимального, что в свою очередь может привести к появлению эффективных криптографических атак.

В ходе проведенных исследований были оценены все длины периодов формируемой последовательности для полей $GF(2^3)$, $GF(2^2)$ при всех возможных состояниях *i* и *j* для всех значений S-боксов, результаты исследований приведены на рис.3,4.

Количество периодов

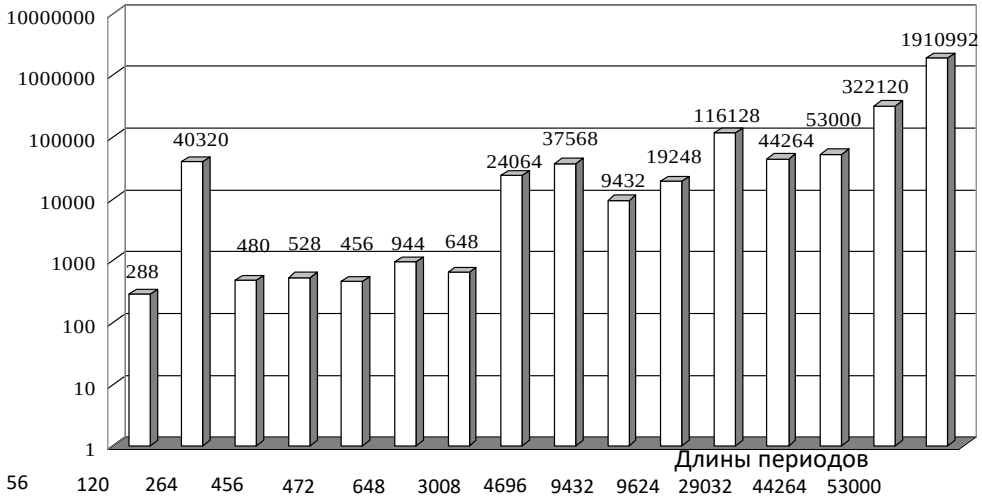

Рис.3. Распределения числа периодов для поля $GF(2^3)$ при полном переборе значений i и j

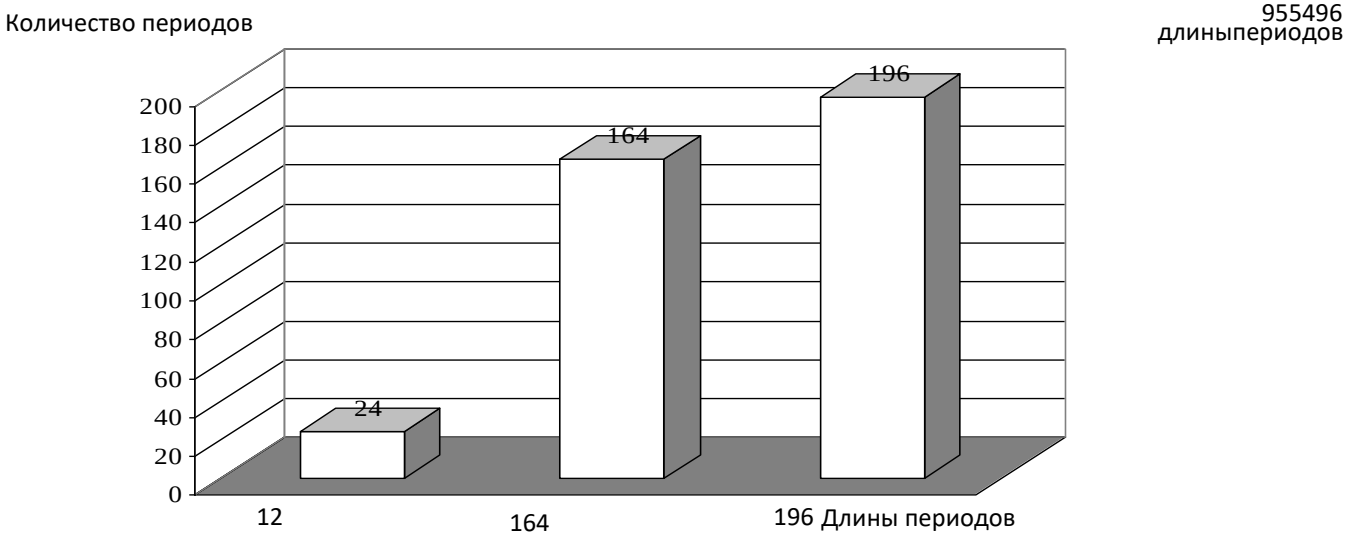

Рис.4. Распределения числа периодов для поля $GF(2^2)$ при полном переборе значений i и j

Таким образом, в ходе проведенных исследований выявлено что для каждого *S*-бокса существует значения *i* и *j*, при которых длина периода строго определена.

Так для S-боксов из поля $GF(2^2)$ (их количество равно $4!=24$) длина периода составляет 12 элементов последовательности, а для S-боксов из поля $GF(2^3)$ (их количество равно $8!=40320$) длина периода составляет 56 элементов последовательности.

На основе проведенных исследований периодических свойств ГПСЧ RC4 авторами предлагается комбинирующий генератор структурная схема которого представлена на рис. 5, блок-схема – на рис.6. Основным отличием от известной схемы ГПСЧ RC4 является неравенство ключевых последовательностей $I_1 \neq I_2, J_1 \neq J_2$.

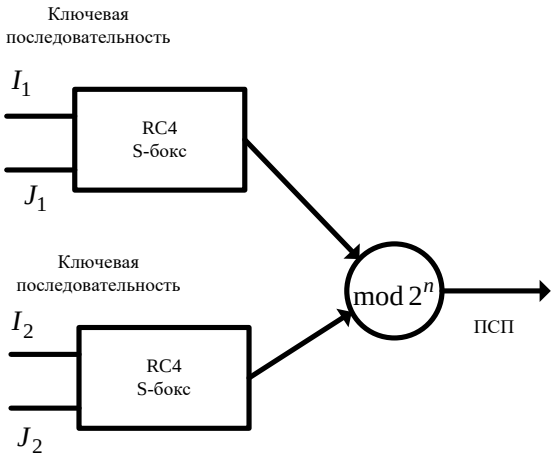

Рис.5. Комбинирующий генератор

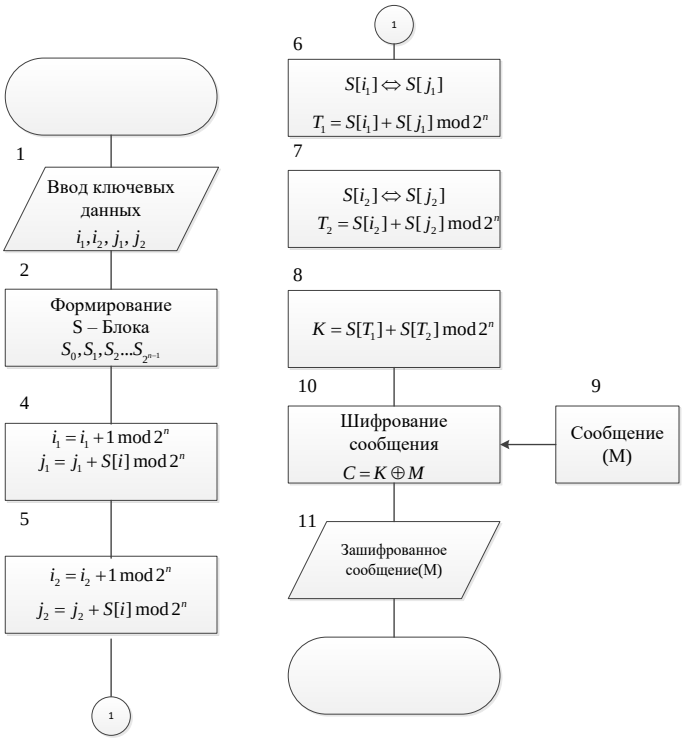

Рис.6. Блок-схема предлагаемого комбинирующего ГПСЧ

На рис. 7 представлены результаты исследования статистической безопасности предложенного комбинирующего генератора на основе ГПСЧ RC4 по методике NIST STS 822. Статистический портрет подтверждает криптостойкость предложенного генератора.

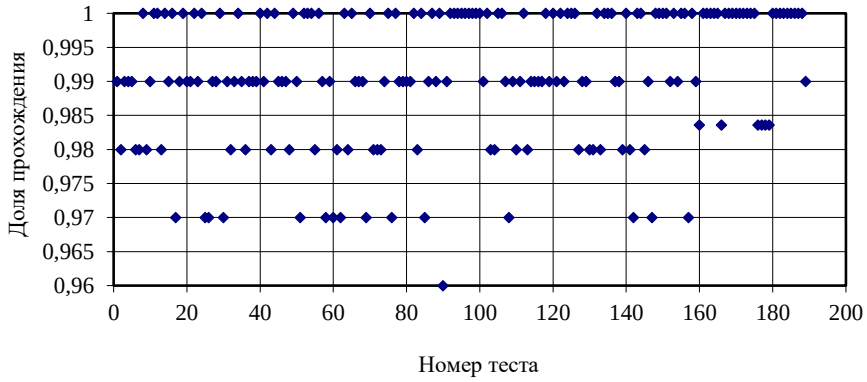

Рис. 7. Статистический портрет предложенного комбинирующего генератора на основе ГПСЧ RC4

Выводы и перспективы дальнейших исследований. Проведенные исследования показали, что генератор ППСЧ на основе алгоритма RC4 при ключевых значениях $I, J \neq 0$ не обеспечивает требуемый уровень криптостойкости сгенерированной ПСП из-за малого периода (период формирования ППСЧ на несколько порядков ниже максимального). Для устранения выявленной коллизии предлагается использование комбинации из двух и более ГПСЧ RC4, что дает возможность увеличить количество ключевых последовательностей на одном S-боксе.

Литература:

1. Шнайер Б. Прикладнаякриптография. Протоколы, алгоритмы, исходныетексты на языкеСи. – М.: Издательство ТРИУМФ, 2002, 816 с.

2. ПоточныешифрыРезультатызарубежнойоткрытойкриптологии [Електронний ресурс] // –М. 1997 – режим доступа : www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm Москва 1997.

3. Рябко Б.Я. Криптографическиеметодызащитыинформации /Б. Я. Рябко, А.Н. Фионов. – М.: Гарячаялиния-Телеком, 2005. 229 с.

4. Анализобобщенияалгоритма RC4 [Електронний ресурс] //–М. 2009 – режим доступа : www.vniipvti.ru/data/file/sbor3_11.pdf

5. Євсеєв С. П. Використання міні-версій для оцінки стійкості блоково-симетричних шифрів / С. П. Євсеєв, С. Е. Остапов, Р. В. Корольов // Науково-технічний журнал "Безпека інформації". том.23. № 2. Київ. – 2017. – с. 100 – 108.

6. И.Д. Горбенко"Новаяидеологияоценкистойкостиблочныхсимметричныхшифров к атакам дифференциального и линейного криптоанализа"Прикладнаярадиоэлектроника. Том 9, № 3, С. 312 – 320, 2010.

7. В.И. Долгов, И.В. Лисицкая "Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа": монография, Харьков: Издательство «Форт», 420 с., 2013.

8. И.В. Лисицкая "О новойметодикеоценкистойкостиблочныхсимметричныхшифров к атакам дифференциального и линейного криптоанализа" Системи обробки інформації. Вип. 4 (94), С. 167-173, 2011.

9. И.В. Лисицкая "Методологияоценкистойкостиблочныхсимметричныхшифров" [Электронный ресурс] .– Режим доступа : https://cyberleninka-.ru/article/n/metodologiya-otsenki-stoykosti-blochnyh-simmetrichnyh-shifrov.

10. И.В. Лисицкая "Большиешифры – случайныеподстановки. Сравнениедифференциальных и линейныхсвойствшифров, представленных на украинский конкурс, и ихуменьшенных моделей" / [Электронный ресурс]. – Режим доступа: https://cy-berleninka.ru/article/n/bolshie-shifry-sluchaynyepod-stanovki-sravnenie-differentsialnyh-i-lineynyh-svoystv-shifrov-predstavlennyh-na-ukrainskiy-konkurs-i-ih.

11. И.В. Лисицкая, К.Е. Лисицкий, М.Ю. Родинко, И.А. Головко, И.И. Жариков, М.А. Корниенко, М.В. Кулеба "Эксперементальныеданные по определениюдинамическихпоказателейприходаблочныхсимметричныхшифров к состояниюслучайности" Радіоелектроніка, інформатика, управління, № 1, С. 129 – 141, 2017.

12. И.В. Лисицкая, А. А. Настенко "Большиешифры – случайныеподстановки". Межведомственныйнаучн. техническийсборник «Радиотехника», вып. 166, С. 50–55, 2011.

13. Л. Сорока, А. Кузнецов, И. Московченко, С. Исаев "Исследование дифференциальных свойств блочно-симметричных шифров", Системиобробкиінформації. Вип. 6 (87), С. 286-295, 2010.

14. И. Лисицкая, А. Кузнецов, С. Исаев “Линейные свойства блочных симметричных шифров, представленных на украинский конкурс”,Прикладная радиоэлектроника: научно-техн. журнал. Том 10,№ 2, С. 135-140, 2011.

15. И.В. Лисицкая, Т.А. Гриненко, С.Ю. Бессонов “Анализдифференциальных и линейныхсвойствшифровrijndael, serpent, threefish при 16-битных входах и выходах” Восточно-Европейский журнал передовыхтехнологий, С. 50-54, 2015.

16. В.И. Долгов, Р.В. Олейников, А.Ю. Большаков “Криптографическиесвойствауменьшеннойверсиишифра «Калина»” Прикладнаярадиоэлектроника, Том 9, № 3, С. 349-354, 2010.

17. G. Piret, F.-X. Standaert “Provablesecurityofblockciphersagainstlinearcryptanalysis: a missionimpossible?” Designs, CodesandCryptography. V. 50,N 3, P. 325 – 338, 2009.

18. B. Collard, F.-X. Standaert “Experimentinglinearcryptanalysis” AdvancedLinearCryptanalysis. V.116, P. 90-117, 2011.

19. L.R. Knudsen “Practically Secure Feistel Ciphers”. Proc. FastSoftwareEncryption, Cambridge, 1993, Springer, V.809, P. 211-221, 1994.

20 І.Д. Горбенко, В.І. Долгов, Р.В. Олійников “Перспективний блоковий симетричний шифр «КАЛИНА». Основні положення та специфікація” Прикладнаярадиоэлектроника. Т. 6, № 2, С. 195-208, 2007.

21. І.Д. Горбенко, В.І. Долгов, Р.В. Олійников “Перспективний блоковий симетричний шифр «Мухомор». Основні положення та специфікація” Прикладнаярадиоэлектроника. Т. 6, № 2, С. 147-157, 2007.

22. Головашич С.А. “Спецификацияалгоритма блочного симметричногошифрования «Лабиринт»” Прикладнаярадиоэлектроника. Т. 6, № 2, С. 230-240, 2007.

23. И.В. Лисицкая “Сравнение по эффективностисуперблоковнекоторыхсовременныхшифров” Радіоелектроніка, інформатика, управління. № 1, С. 37 – 44, 2012.

Рецензент: д.т.н., проф. Дудикевич В.Б. Поступила 21.08.2018

Євсеєв С.П., Корольов Р.В., Белоус Д.М

РЕЗУЛЬТАТИ ОЦІНКИ ПЕРІОДИЧНИХ ВЛАСТИВОСТЕЙ S-BOX АЛГОРИТМА ПОТОКОВЕ ШИФРУВАННЯ RC4

В роботі проведені дослідження періодичних властивостей послідовностей псевдовипадкових чисел, що формуються генератором RC4. проведені дослідження формування S-box для алгоритму шифрування Rc-4 показали, що розглянутий генератор володіє "слабкими" ключами, використання яких призводить до формування послідовностей псевдовипадкових чисел з малим періодом, що в свою чергу може привести до успішних криптографічним атакам.

Ключові слова: генератор псевдовипадкових чисел, потоковий шифр, криптографічні атаки, міні-версія криптоалгоритма.

Yevseiev S., Korolev R., Belous D.

RESULTS OF ESTIMATION OF PERIODICAL PROPERTIES OF S-BOX ALGORITHM OF RC4 FINAL SCREENING

In the articleinvestigates the periodic properties of sequences of pseudo-random numbers generated by the RC4 generator. The conducted studies of S-box formation for the Rc-4 encryption algorithm showed that the considered generator has "weak" keys, the use of which leads to the formation of sequences of pseudo-random numbers with a short period, which in turn can lead to successful cryptographic attacks.

Keywords:a pseudo-random number generator, a stream cipher, cryptographic attacks, a mini version of the cryptoalgorithms.