Подход к построению потоковых шифров с применением генератора псевдослучайных последовательностей, основанного на нечеткой логике

И.В. Аникин[1], *Х.Х. Альнаджар*[2]

[1]*Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, Казань, Россия*
[2]*Высший институт прикладных наук и технологий, Дамаск, Сирия*

Аннотация: Предложен подход к потоковому шифрованию данных, основанный на использовании нового типа генераторов гаммы шифра с нелинейной функцией выбора регистра сдвига, основанной на нечеткой логике. Подобраны наилучшие конфигурации генератора для формирования гаммы, свойства которой наиболее близки к свойствам белого шума. Показано, что предложенный подход позволяет осуществлять генерацию гамма последовательности с качеством, превышающим ряд других классических генераторов.

Ключевые слова: криптография, потоковый шифр, гамма шифра, генератор псевдослучайных последовательностей, тест случайности, нечеткая логика, функция принадлежности, лингвистическая переменная, дефаззификация, регистр сдвига с линейной обратной связью.

Введение

Вопрос обеспечения конфиденциальности представляет высокую актуальность для множества протоколов передачи данных, используемых в различных предметных областях [1]. Для его решения применяются разнотипные криптографические преобразования (алгоритмы), выполняющие обратимое зашифрование данных, основанное на ключе [2]. В симметричных криптосистемах зашифровка и расшифровка данных осуществляются на одном и том же ключе, являющемся секретным. С другой стороны, асимметричные криптосистемы используют пару ключей. Открытый ключ используют для зашифровки данных, а секретный ключ - для обратного преобразования. Знание открытого ключа не позволяет выполнить расшифрование данных либо узнать секретный ключ за приемлемое время.

Различают блочные и потоковые криптографические алгоритмы (шифры) [3]. Блочный шифр выполняет зашифрование данных, деля их на блоки фиксированной длины. Наиболее распространенные варианты построения блочных шифров используют SP-сети и сети Фейстеля. В

качестве основных режимов шифрования используются: режим электронной кодовой книги (ECB), режим сцепления шифрблоков (CBC), режим обратной связи по шифртексту (CFB), режим обратной связи по выходу (OFB). К наиболее известным симметричным блочным шифрам относят DES, AES, ГОСТ 28147-89, Магма, Кузнечик, Blowfish, FEAL, CAST-128 и др.

Потоковые шифры

Потоковые шифры представляют собой иной класс симметричных криптографических алгоритмов, в которых элементы открытого текста преобразуются в элементы шифртекста, учитывая место их расположения в исходном потоке. Работа потоковых шифров основана на формировании длинных непредсказуемых битовых последовательностей со свойствами, близкими к белому шуму (гаммы шифра, представляющей собой ключевой поток) [4]. Для их формирования используются генераторы псевдослучайных последовательностей (ГПСП) [5,6]. Общая схема потокового шифрования данных представлена на рис. 1. При этом, ГПСП, формирующая ключевой поток, делает это в соответствии с заданным ключом. Этот же ключ используется для формирования ключевого потока на стороне приемника.

К наиболее известным потоковым шифрам относят RC4, A5, SEAL, CryptMT и др. Данные алгоритмы нашли широкое применение в протоколах передачи данных, используемых в сетях мобильной и беспроводной связи (протоколы GSM, WEP, WPA), для обеспечения конфиденциальности аудио- и видеопотоков.

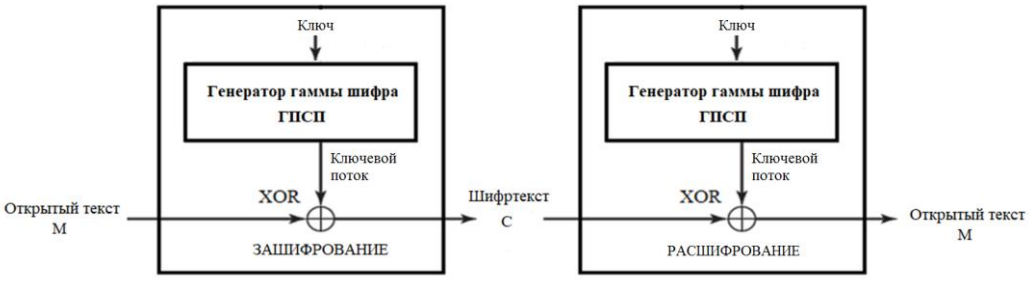

Рис. 1. – Общая схема потокового шифрования данных

Алгоритм RC4 работает по следующему принципу.

1. Формирование S-блока путем перемешивания прямой последовательности чисел в соответствии с криптографическим ключом *K*.

2. Генерация гаммы шифра (ключевого потока) в соответствии со схемой, приведенной на рис. 2.

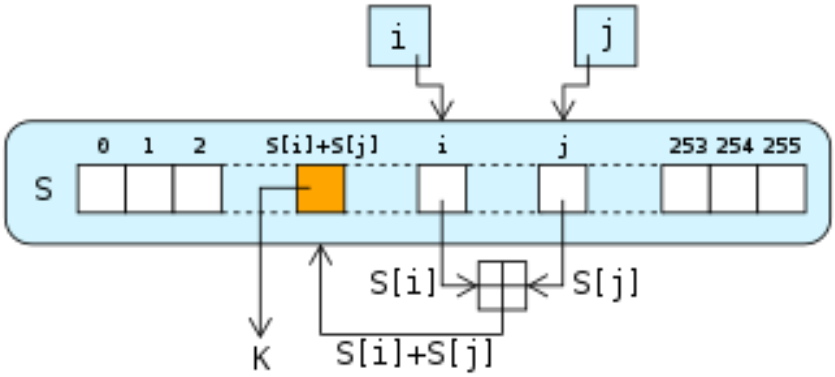

Рис. 2. – Общая схема формирования ключевого потока

Алгоритм A5/1 использует 3 регистра сдвига с линейной обратной связью для формирования гаммы шифра. Его структура представлена на рис. 3. Общий принцип работы алгоритма заключается в следующем.

1. Формируются 19-разрядный (R1), 22-разрядный (R2) и 23-разрядный регистры (R3), представленные на рис. 3.

2. Регистры инициализируются при участии 64-битного ключа и номеров кадра.

3. Формируется гамма шифра в соответствии со схемой, представленной на рис. 3 и зашифрование сообщения в соответствии со схемой, представленной на рис. 1. Управление тактированием осуществляется с помощью битов синхронизации регистров x(R1), y(R2), z(R3), а также булевой функции F=x&y|x&z|y&z. Осуществляется сдвиг регистров с битом синхронизации, совпадающим с F.

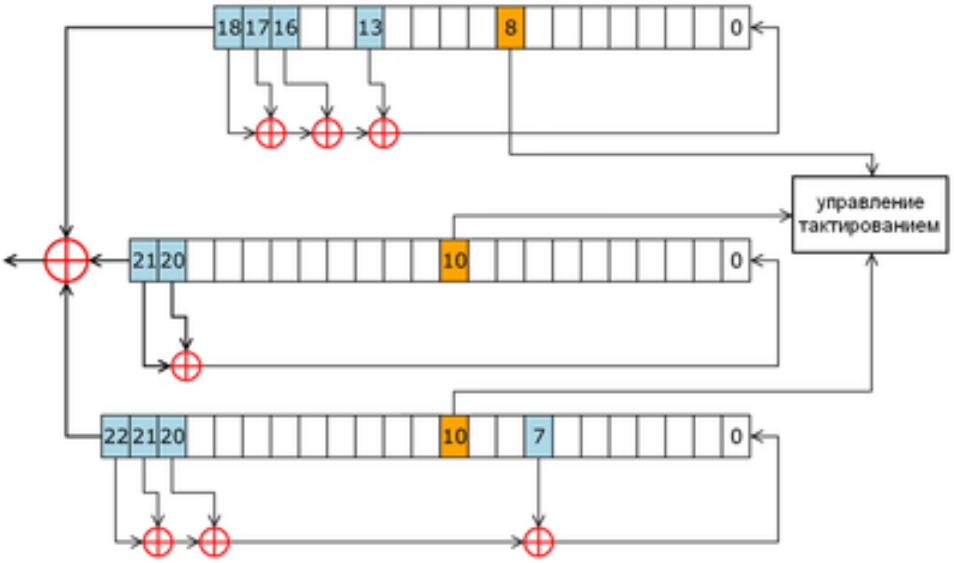

Рис. 3. – Формирование гаммы шифра в алгоритме A5/1

Одной из важнейших задач при построении потоковых шифров является формирование качественной гаммы. Формируемая гамма шифра должна быть близка к истинно случайной, должна быть непредсказуемой, иметь большой период и удовлетворять криптографическим свойствам безопасности [7]. Формируемая гамма шифра должна успешно проходить статистические тесты, представленные в пакетах NIST STS и DIEHARD.

Регистры сдвига с линейной обратной связью (РСЛОС) обладают высоким быстродействием и достаточно часто используются для формирования гаммы шифра. Формируемые ими бинарные последовательности обладают хорошими статистическими свойствами, если соответствующий им характеристический полином является примитивным. ГПСП, основанные на РСЛОС, являются наиболее быстрыми генераторами псевдослучайных последовательностей с большим периодом. Они также требуют небольших аппаратных затрат для реализации. Однако, значительным недостатком РСЛОС является их линейность, что ведет к проблемам безопасности. Для их устранения необходимо использовать

сложную нелинейную функцию с целью перемешивания выходов нескольких РСЛОС.

В данной работе для формирования ГПСП предлагается использование авторского генератора с несколькими РСЛОС и функцией выбора, основанной на применении методов теории нечетким множеств (НГПСП).

Структура генератора

Структура НГПСП предложена авторами статьи в работе [8], представлена на рис. 4 и включает в себя n РСЛОС ($n \geq 2$), n буферов фиксированного размера, принимающих выходные биты соответствующих РСЛОС, а также нелинейную функцию выбора, основанную на применении методов теории нечетким множеств [9]. Нелинейная функция включает в себя две лингвистические переменные (ЛП), блок нечетких ЕСЛИ-ТО правил и блок дефаззификации.

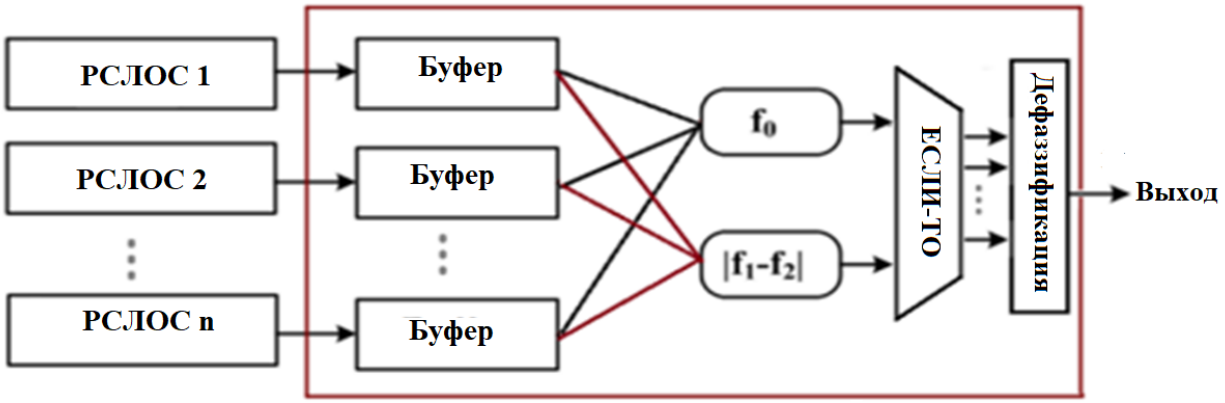

Рис. 4. – Структура НГПСП

Лингвистические переменные используются для анализа статистических свойств буферов. Первая ЛП осуществляет оценку в них числа единиц (f_0). Вторая ЛП ($|f_1-f_2|$) осуществляет оценку разницы между блоками вида (0110) (f_1), и блоками вида (1001) (f_2). Исходные значения функций принадлежности (ФП) ЛП для размера буфера = 8, представлены на рис. 5.

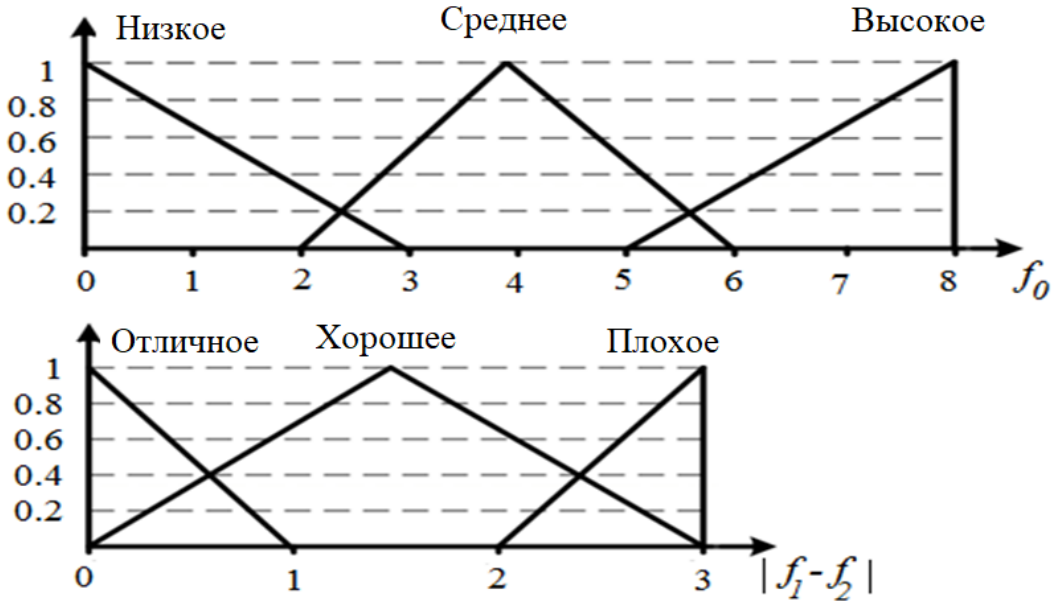

Рис. 5. – Исходные значения ФП ЛП

ЕСЛИ-ТО правила (таблица 1) предназначены для оценки состояния буферов и выбора наилучшего РСЛОС в конкретный момент времени. Последний бит наилучшего РСЛОС подается на выход НГПСП.

Таблица № 1

Конфигурация правил ЕСЛИ-ТО, используемая для выбора РСЛОС

MF	Низкое	Среднее	Высокое
Отличное	Плохое	Лучшее	Плохое
Хорошее	Хорошее	Хорошее	Хорошее
Плохое	Плохое	Хорошее	Плохое

Конфигурирование НГПСП

Качество работы НПГСП напрямую зависит от его конфигурации - выбора значений ряда его параметров. Данные параметры были разделены на две группы. Первая группа содержит один параметр, связанный с используемыми РСЛОС и их характеристическими полиномами. Вторая группа включает несколько параметров, связанных с реализацией нелинейной функции выбора.

Выбранные РСЛОС должны гарантировать максимальный период

генерируемых последовательностей, а также обеспечивать их случайную природу. Для проектирования НГПСП авторами был использован специальный вид примитивных полиномов, определяемых выражением (1) [10]:

$$P(x)=(1+x^{b1})\,(1+x^{b2})\ldots\,(1+x^{bm})+x^{n} \quad (1)$$

где числа $b1,\ldots,bm,n$ должны удовлетворять следующим условиям:

$$b1 \geq 1,\ b1 < b2,\ (b1+b2) < b3,\ldots,\ (b1+\ldots+bm) < n$$

Рассмотрим процесс формирования НГПСП с двумя РСЛОС. Для него были выбраны следующие характеристические полиномы, позволяющие формировать гамму шифра с периодом $T=T^{1}\cdot T^{2}=(2^{89}-1)(2^{97}-1)\approx 10^{56}$:

$$P_1(x)=(1+x)\,(1+x^{5})(1+x^{10})(1+x^{17})(1+x^{39})+x^{89} \quad (2)$$

$$P_2(x)=(1+x)\,(1+x^{4})(1+x^{7})(1+x^{20})(1+x^{53})+x^{97}$$

Рассмотрим следующие параметры НГПСП, связанные с реализацией нелинейной функции НГПСП с двумя РСЛОС: длина буферов, число термов лингвистических переменных f_0, $|f_1-f_2|$, тип и конфигурация их функций принадлежности, используемые ЕСЛИ-ТО правила. При инициализации НГПСП были использованы следующие значения параметров: размер буфера=8, три терма для каждой ЛП – “Low”, “Medium”, “High” для ЛП f_0 и “Excellent”, “Good”, “Bad” для ЛП $|f_1-f_2|$ (рис. 3). Система ЕСЛИ-ТО правил представлена в таблице 1. В таблице 2 представлены правила дефаззификации результата, где Bit1 соответствует LSB буфера, ассоциированного с РСЛОС1, Bit2 соответствует LSB буфера, ассоциированного с РСЛОС2.

Таблица № 2

Правила дефаззификации результата

РСЛОС2\РСЛОС1	Наилучшее	Хорошее	Плохое
Наилучшее	Bit1	Bit2	Bit2
Хорошее	Bit1	Bit1	Bit2
Плохое	Bit1	Bit1	Bit1

После инициализации НГПСП путем задания приведенной выше конфигурации, был осуществлен тюнинг параметров с целью нахождения наилучших их значений, позволяющих формировать наиболее качественную гамму шифра. Оценка и поиск наилучших значений параметров осуществлялись путем тестирования сгенерированных последовательностей с помощью пяти наиболее значимых тестов случайности, входящих в пакет NIST, и выделенных авторами в работе [11]. Значения параметров НГПСП, при которых формировалась наилучшая последовательность, выбирались в качестве искомых. В таблице 3 представлены найденные наилучшие значения параметров НГПСП. Финальный генератор успешно прошел все тесты случайности, включенные в пакеты NIST и DIEHARD.

Таблица № 3

Конфигурация НГПСП, полученная в результате тюнинга

Параметр НГПСП	Значение
Характеристические полиномы	Определяются выражением (2)
Размер буферов	32
Число термов для ЛП (f_0, $\|f_1-f_2\|$)	(3,3)
Тип функций принадлежности	Трапециидальные
Конфигурация ФП для ЛП f_0 в РСЛОС1	Низкое: {0,...,9}, Среднее:{10,...,20}, Высокое:{21, ..., 32}
Конфигурация ФП для ЛП $\|f_1-f_2\|$ в РСЛОС1	Отличное:{ 0, ..., 2}, Хорошее:{3, 4}, Плохое: {5,...10}
Конфигурация ФП для ЛП f_0 в РСЛОС2	Низкое: {0, ..., 11}, Среднее: {12, ..., 18}, Высоке: {19, ..., 32}
Конфигурация ФП для ЛП $\|f_1-f_2\|$ в РСЛОС2	Отличное: {0, 1}, Хорошее: {2, 3}, Плохое: {4, ..., 10}

Исследование НГПСП

Был исследован вопрос: является ли использование малого количества длинных РСЛОС лучшим для генерации качественной гаммы шифра, чем

использование большого количество относительно коротких РСЛОС. Для ответа на данный вопрос было проведено исследование двух генераторов: 1) НГПСП с двумя РСЛОС, конфигурация которого определена в таблице 3; 2) НГПСП с четырьмя РСЛОС, имеющих следующие примитивные характеристические полиномы: $P_1(x)=(1+x)(1+x^4)(1+x^{10})(1+x^{19})+x^{37}$, $P_2(x)=(1+x)(1+x^6)(1+x^9)(1+x^{22})+x^{41}$, $P_3(x)=(1+x)(1+x^2)(1+x^7)(1+x^{11})+x^{47}$, $P_2(x)=(1+x^2)(1+x^8)(1+x^{14})(1+x^{27})+x^{59}$

Был осуществлен тюнинг параметров второго НГПСП.

Итоговые генераторы прошли все тесты NIST и DIEHARD. Однако, в ходе исследования последовательностей, формируемых данными генераторами, была обнаружена различная их стойкость к корреляционным атакам. Вероятности появления длинных подпоследовательностей, состоящих только из единиц либо нулей, может быть относительно высокой для одного из РСЛОС. В этом случае нелинейная комбинационная функция будет выбирать выход другого РСЛОС в качестве выхода генератора. Как итог, использование двух РСЛОС может вести к уязвимостям НГПСП по отношению к корреляционным атакам. Для второго НГПСП, имеющего большее количество более коротких РСЛОС, стойкость к корреляционным атакам является более высокой. Это происходит в связи с более высокой частотой переключения между РСЛОС и меньшей вероятностью формирования длинных подпоследовательностей, состоящих только из единиц или нулей. Таким образом, второй НГПСП является более предпочтительным, а увеличение количества РСЛОС ведет к увеличению качества генерируемых гамма последовательностей.

Исследован профиль линейной сложности нелинейной функции НГПСП, конфигурация которого определяется таблицей 3. Эта сложность определяется минимальной длиной РСЛОС, который может генерировать бинарную последовательность. Кривая профиля линейной сложности

является одной из важнейших характеристик, используемой при оценке случайности конечной последовательности. Она представляет собой непредсказуемую последовательность длины *n* над полем *GF(2)*, которая должна быть близка к линии *n/2*. Кривая профиля линейной сложности случайной последовательности должна выглядеть, как «беспорядочная лестница» с длиной шага (≈ 4) и высотой шага (≈ 2). Любые регулярные характеристики должны быть исключены. Оценка кривой профиля линейной сложности для длинной последовательности (≈ 1 Mbits), сгенерированной НГПСП, показала удовлетворение вышеперечисленным свойствам.

Было произведено сравнение качества работы НГПСП, конфигурация которого определяется таблицей 3, с 21 другим генератором: 16 ГПСЧ, входящих в состав DIEHARD и 5 ГПСЧ, реализованных в различных языках программирования. Каждым ГПСЧ были сформированы гамма последовательности длиной 1Мбит. Данные последовательности были протестированы с помощью 5 наиболее значимых тестов NIST с использованием двух статистических критериев (X^2 и числа подпоследовательностей, проваливших тесты). Предложенный НГПСП получил наилучшие результаты в ходе тестирования. Таким образом, его применение в потоковых шифрах является предпочтительным.

Выводы

Предложен подход к формированию гаммы для потоковых шифров. Подход основан на использовании нового типа генератора псевдослучайных последовательностей с нелинейной функцией выбороа, основанной на нечеткой логике. Преимуществом предложенного подхода к построению ГПСП является возможность тюнинга параметров НГПСП для генерации гаммы шифра с наилучшими статистическими свойствами. Были исследованы параметры предложенного НГПСП и найдены наилучшие значения для них, позволяющие формировать наилучшие гамма-

последовательности. Была исследована стойкость различных генераторов к корреляционным атакам и даны рекомендации использовать НГПСП с большим количеством РСЛОС для устранения возможных уязвимостей. Предложенный НГПСП был сравнен с 21 другими широко известными генераторами. Исследование показало, что НГПСП формирует гамма последовательности с более хорошими статистическими свойствами. НГПСП может быть использован, как элемент формирования гамма-последовательностей в потоковых шифрах.

Для реализации потокового шифра, основанного на НГПСЧ, может быть использована схема, представленная на рис. 1. При этом ключ шифрования может быть использован для инициализации РСЛОС НГПСП, аналогично алгоритму A5/1.

В работе был использован специальный тип примитивных полиномов РСЛОС с малым энергопотреблением и малой стоимостью аппаратной реализации. Это делает возможным использование НГПСП как встроенного элемента различных устройств, используемых в киберфизических системах.

Литература

1. Москвин А.Д., Петросян Л.Э. Анализ современных алгоритмов шифрования данных // Инженерный вестник Дона, 2023, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2023/8323

2. Куликова О.В., Пиневич Е.В., Домбаян Г.С., Егоров Н.В., Волохов А.С. Оценка защищенности информации при передаче данных между субъектами доступа в клиент-серверной архитектуре // Инженерный вестник Дона, 2021, № 4 URL: ivdon.ru/ru/magazine/archive/n4y2021/6900

3. Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации. СПб: НИУ ИТМО, 2012. 142 с.

4. Урбанович П.П. Защита информации методами криптографии, стеганографии и обфускации. Минск: БГТУ, 2016. 220 с.

5. Песошин В.А., Кузнецов В.М., Кузнецова А.С., Шамеева А.Р. Генераторы псевдослучайных последовательностей немаксимальной длины на регистрах сдвига // Известия высших учебных заведений. Поволжский регион. Технические науки. 2019. № 1 (49). С. 3-17.

6. Песошин В.А., Кузнецов В.М., Кузнецова А.С. Генераторы псевдослучайных последовательностей немаксимальной длины на регистрах сдвига с линейной обратной связью на основе примитивного многочлена в степени // Известия высших учебных заведений. Поволжский регион. Технические науки. 2019. № 4 (52). С. 14-26.

7. Rueppel R.A. Analysis and Design of Stream Ciphers. Berlin, Heidelberg Springer-Verlag, 1986. 244 p.

8. Anikin I.V., Alnajjar K. Pseudo-random number generator based on fuzzy logic // Proceedings of International Siberian Conference on Control and Communications (SIBCON). 2016. pp. 1-4.

9. Zimmermann H.J. Fuzzy set theory - and its applications. 2nd ed. Springer Science+Business Media, LLC. 1991. 408 p.

10. Anikin I.V., Alnajjar K. Primitive Polynomials Selection Method for Pseudo-Random Number Generator Based on Fuzzy Logic // Proceedings of IEEE Dynamics of Systems, Mechanisms and Machines (Dynamics). 2017. pp. 1-4.

11. Anikin I.V., Alnajjar K. Increasing the quality of pseudo-random number generator based on fuzzy logic generator. Journal of Physics: Conf. Series. 2019, 1096. Pp. 1-7.

12. Knuth D. E. The Art of Computer Programming: Semi-numerical algorithms. Addison-Wesley publishing company. 1968. 624 p.

References

1. Moskvin A.D., Petrosjan L.Je. Inzhenernyj vestnik Dona, 2023, № 4. URL: www.ivdon.ru/ru/magazine/archive/n4y2023/8323.

2. Kulikova O.V., Pinevich E.V., Dombajan G.S., Egorov N.V., Volohov A.S. Inzhenernyj vestnik Dona, 2021, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2021/6900.

3. Gatchenko N.A., Isaev A.S., Jakovlev A.D. Kriptograficheskaja zashhita informacii [Information protection with using cryptography]. SPb: NIU ITMO, 2012. 142 p.

4. Urbanovich P.P. Zashhita informacii metodami kriptografii, steganografii i obfuskacii [Information protection with using cryptography, steganography and obfuscation]. Minsk: BGTU, 2016. 220 p.

5. Pesoshin V.A., Kuznecov V.M., Kuznecova A.S., Shameeva A.R. Izvestija vysshih uchebnyh zavedenij. Povolzhskij region. Tehnicheskie nauki. 2019. № 1 (49). pp. 3-17.

6. Pesoshin V.A., Kuznecov V.M., Kuznecova A.S. Izvestija vysshih uchebnyh zavedenij. Povolzhskij region. Tehnicheskie nauki. 2019. № 4 (52). pp. 14-26.

7. Rueppel R.A. Analysis and Design of Stream Ciphers. Berlin, Heidelberg Springer-Verlag, 1986. 244 p.

8. Anikin I.V., Alnajjar K. Proceedings of International Siberian Conference on Control and Communications (SIBCON). 2016, pp. 1-4.

9. Zimmermann H.J. Fuzzy set theory - and its applications. 2nd ed. Springer Science+Business Media, LLC. 1991. 408 p.

10. Anikin I.V., Alnajjar K. Proceedings of IEEE Dynamics of Systems, Mechanisms and Machines (Dynamics). 2017, pp. 1-4.

11. Anikin I.V., Alnajjar K. Journal of Physics: Conf. Series. 2019. 1096. pp. 1-7.

12. Knuth D. E. The Art of Computer Programming: Semi-numerical algorithms. Addison-Wesley publishing company. 1968. 624 p.