УДК 004.056.55
DOI: 10.18413/2518-1092-2021-6-2-0-2

Буханцов А.Д.[1]
Саджид А.Ю.[1]
Устинов А.Н.[1]
Родионов С.В.[2]

ИССЛЕДОВАНИЕ НАДЁЖНОСТИ ШИФРОВАНИЯ РЕЧИ В ТЕХНОЛОГИИ МОБИЛЬНОЙ СВЯЗИ GSM

[1] Белгородский государственный национальный исследовательский университет, ул. Победы д. 85, г. Белгород, 308015, Россия
[2] Украинский государственный университет железнодорожного транспорта, пл. Фейербаха, д. 7, г. Харьков, 61050. Украина

e-mail: bukhantsov@bsu.edu.ru, 1275117@bsu.edu.ru, 1319385@bsu.edu.ru, rodionov.serhii@kart.edu.ua

Аннотация
В статье проводится анализ стойкости алгоритма поточного шифра A5/1 в системе сотовой связи GSM на основе разработанной программы моделирования процесса формирования ПСП комбинированной схемой из линейных регистров и реализованного в программной среде MatLab статистического теста FIPS 140 – 1 / FIPS 140 – 2. Результаты анализа позволяют установить, что последовательность, формируемая на основе комбинированной схемы из ЛРР A5/1, не является псевдослучайной, что может позволить выработать рекомендации по дальнейшему совершенствованию механизма защиты в данной системе мобильной связи.
Ключевые слова: шифрование, алгоритм A5/1, сеть GSM, аутентификация.
Для цитирования: Буханцов А.Д., Саджид А.Ю., Устинов А.Н., Родионов С.В. Исследование надёжности шифрования речи в технологии мобильной связи GSM // Научный результат. Информационные технологии. – Т.6, №2, 2021 – С. 9-17. DOI: 10.18413/2518-1092-2021-6-2-0-2

Buhantsov A.D.[1]
Sadjiid A.Yu.[1]
Ustinov A.N.[1]
Rodionov C.V.[2]

RESEARCH OF SPEECH ENCRYPTION RELIABILITY IN GSM MOBILE COMMUNICATION TECHNOLOGY

[1] Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia
[2] Ukrainian State University of Railway Transport 7 Feuerbach Square, Kharkiv, 61050, Ukraine

e-mail: bukhantsov@bsu.edu.ru, 1275117@bsu.edu.ru, 1319385@bsu.edu.ru, rodionov.serhii@kart.edu.ua

Abstract
The article analyzes the strength of the A5/1 stream cipher algorithm in the GSM cellular communication system based on the developed program for modeling the PSP process with a combined circuit of linear registers and the FIPS 140-1 / FIPS 140-2 statistical test implemented in the MatLab software environment. The results of the analysis make it possible to establish that the sequence formed on the basis of the combined scheme from the LRR A5 / 1 is not pseudo-random, which can make it possible to develop recommendations for further improving the protection mechanism in this mobile communication system.
Keywords: encryption, algorithm A5/1, network GSM, authentication.
For citation: Buhantsov A.D., Sadjiid A.Yu., Ustinov A.N., Rodionov C.V. Research of speech encryption reliability in GSM mobile communication technology // Research result. Information technologies. – T.6, №2, 2021. – P. 9-17. DOI: 10.18413/2518-1092-2021-6-2-0-2

ВВЕДЕНИЕ

В настоящее время повсеместно используются беспроводные технологии связи, которые с одной стороны являются удобными в использовании, но с другой стороны увеличивают риски утечки данных, что требует дальнейшего повышения степени защищенности таких технологий. Одной из гарантий надежности внедряемых криптографических алгоритмов является их открытость, которая позволяет экспертному сообществу проводить их анализ и находить слабые места с целью дальнейшего совершенствования их защищенности. Одной из таких систем является стандарт сотовой связи GSM, механизмы защиты которого хорошо известны и широко опубликованы в открытой печати [1, 3-6].

В данной статье рассмотрены принципы организации безопасной передачи информации в системе сотовой связи GSM, проведен процесс моделирования некоторых элементов системы защиты и сформулированы предложения по их совершенствованию.

Одним из алгоритмов шифрования, применяемых в данном стандарте, является поточный шифр A5/1. В свое время он имел ряд преимуществ в обеспечении конфиденциальности беспроводной связи. Для того чтобы понять, насколько данный алгоритм эффективен в наше время, будет проведена оценка стойкости использования данного метода шифрования при помощи моделирования схемы A5/1 и статического теста для генераторов случайных чисел FIPS 140–1 / FIPS 140–2.

ОРГАНИЗАЦИЯ ЗАЩИТЫ СЕТИ GSM

В технологи GSM (Global System for Mobile Communications) элементы безопасности реализуется в трех объектах: SIM-карта, GSM-телефон и сеть. Модуль идентификации абонента (SIM) содержит [3]:

- IMSI – TMSI – PIN;
- Ключ аутентификации *Ki* (64-битный);
- Алгоритм A8 генерации ключа шифрования *Kc*;
- Алгоритм аутентификации *A3*;
- SIM-карта защищена PIN-кодом и принадлежит оператору.

Из этого следует, что техническая безопасность GSM обеспечивается набором алгоритмов, используемых для организации соединения сотового телефона с сетью оператора GSM.

АУТЕНТИФИКАЦИЯ МОБИЛЬНОЙ СТАНЦИИ

Каждый абонент мобильного телефона получает стандартный модуль аутентификации (SIM-карту), который содержит следующие данные на период использования системы связи:

- IMSI (International Mobile Station Indentifer) – международный идентификационный номер мобильного абонента,
- свой индивидуальный ключ аутентификации K_i,
- алгоритм аутентификации *A3*.

Также каждому абоненту системы связи присваивается «временное удостоверение личности» или временный международный идентификационный номер пользователя TMSI (Temporary Mobile Station Indentifer). После завершения процесса аутентификации и запуска режима шифрования временный идентификационный номер – TMSI передается на мобильную станцию, только в зашифрованной форме. Этот номер TMSI используется для всего последующего доступа к системе. Необходимая информация об участниках хранится в базах данных оператора сети участника [4].

С помощью заложенной в SIM информации в результате взаимного обмена данными между мобильной станцией и сетью осуществляется полный цикл аутентификации и разрешается доступ абонента к сети. На рисунке 1 представлена схема аутентификации.

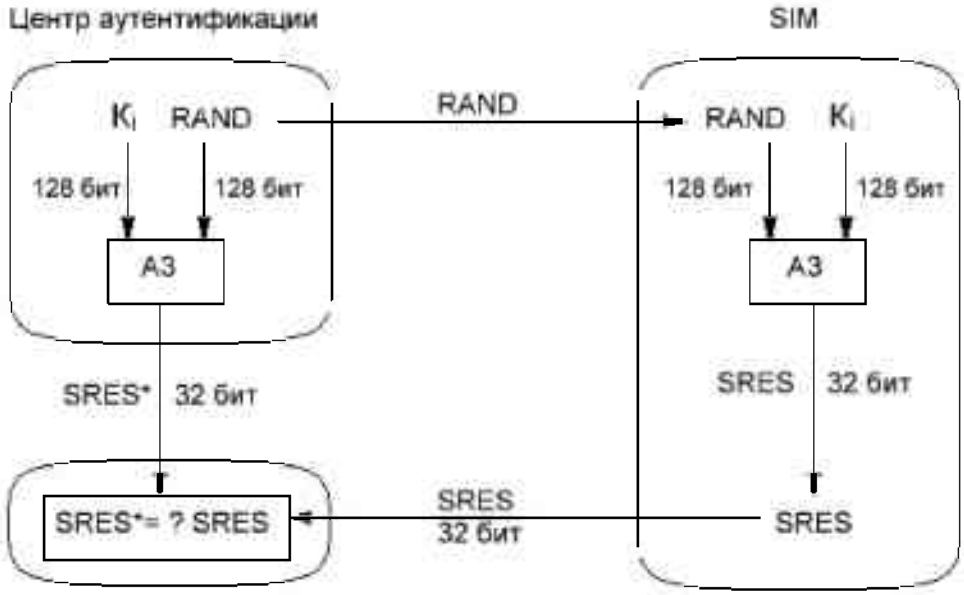

Рис. 1. Схема процесса аутентификации GSM
Fig. 1. GSM authentication Process Diagram

Процесс аутентификации выглядит следующим образом [4]:

- На каждой SIM-карте запрограммирован уникальный ключ аутентификации абонента. Центр аутентификации (ЦА) имеет список, который сопоставляет номер K_i с SIM-картой.
- Когда SIM-карта запрашивает вызов, 128-битное случайное число мгновенно генерируется ЦА и передается на SIM-карту.
- Алгоритм A3, который запрограммирован внутри SIM-карты, обрабатывает число RAND и число K_i, и генерирует 32-битный вывод, называемый подписанным номером ответа (SRES).
- Тот же процесс выполняется на стороне ЦА.
- SIM-карта передает этот номер SRES в ЦА.
- ЦА сравнивает полученный SRES с SRES, сгенерированным на стороне сети.
- SIM-карта аутентифицируется тогда и только тогда, когда два SRES одинаковы.

ШИФРОВАНИЕ В СЕТИ GSM

Сеть GSM использует информацию, хранящуюся на SIM-карте и в телефоне, для обеспечения зашифрованной связи и аутентификации. Шифрование GSM применяется только к связи между мобильным телефоном и базовой станцией. Остальная часть передачи по обычной фиксированной сети или радиорелейной сети не защищена, и ее можно легко перехватить или изменить. Шифрование GSM достигается за счет использования общего секретного ключа. Ключ 64-бит разделен для обеспечения конфиденциальности данных [5]. Невозможно зашифровать все данные; например, некоторая информация о маршруте должна быть отправлена в виде открытого текста. Подробный процесс шифрования данных показан на рисунке 2.

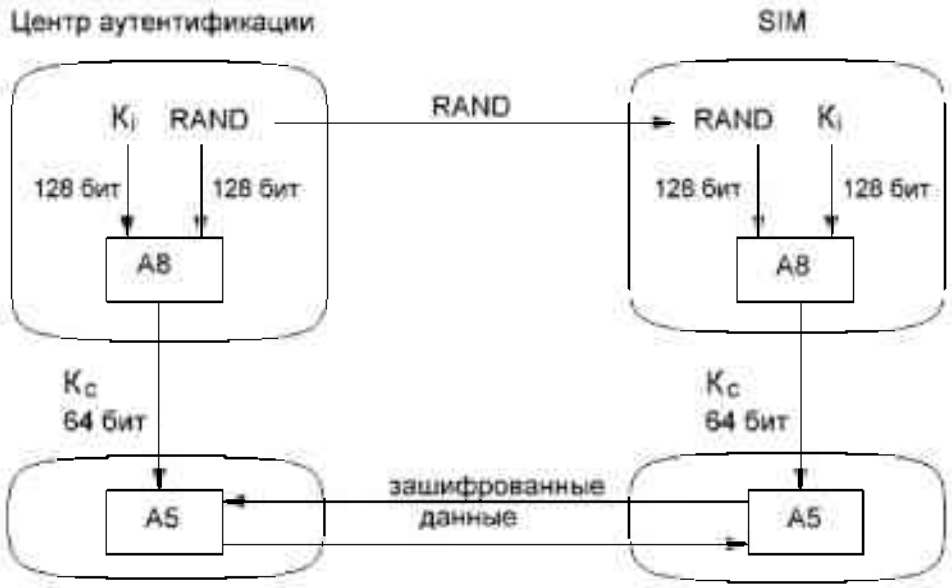

Рис. 2. Схема процесса шифрования GSM
Fig. 2. GSM encryption Process Diagram

Алгоритм выполнения шифрования выглядит следующим образом [4]:

- ЦА генерирует случайное число (RAND) из 128 бит и отправляет его в МС.
- RAND и число *Ki* обрабатываются алгоритмом A8 с обеих сторон. Алгоритм A8 создает 64-битный ключ шифрования *Кс*.
- Алгоритм A5 использует ключ *Кс* при поточном шифровании данных.

В системе мобильной связи стандарта GSM алгоритм шифрования речи A5 использует сложение по модулю-2 данных (после соответствующего преобразования речи в двоичную последовательность) и ПСП (псевдослучайная последовательность), которая вырабатывается комбинированной схемой из ЛЛР с псевдослучайным тактированием [3].

Алгоритм состоит из 3-х линейных регистров сдвига с обратной связью (ЛРОС) длиной 19, 22 и 23. Алгоритм A5 существует в двух модификациях A5 / 2 и A5 / 1.

Рассмотрим подробнее алгоритм A5 / 1.

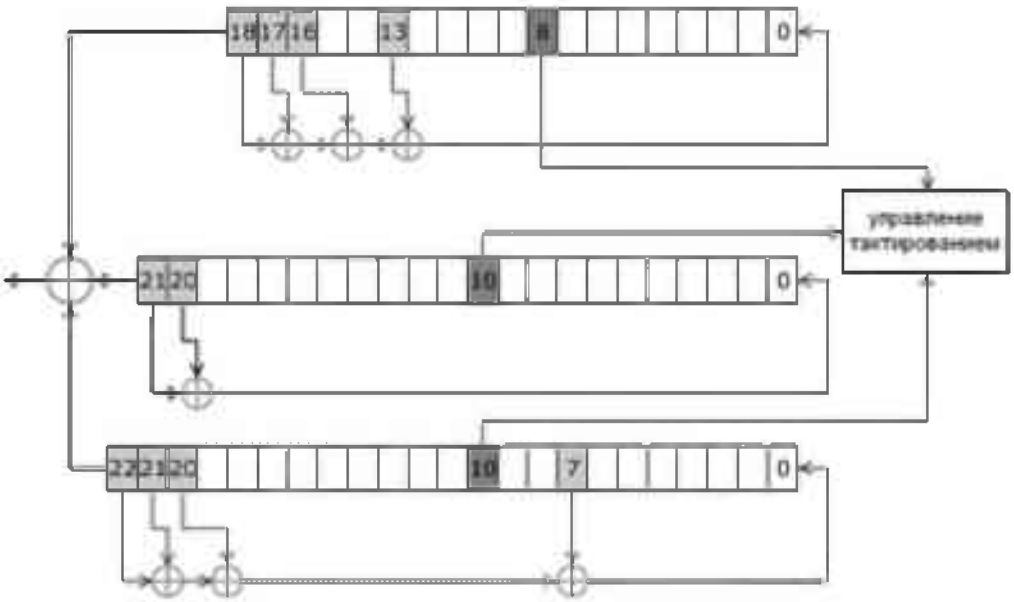

Рис. 3. Алгоритм шифрования A5/1 стандарта GSM
Fig. 3. A5/1 GSM encryption algorithm

Из рисунка 3 видно, что генератор гаммы потокового шифра A5/1 состоит из трех ЛРР, соответствующих примитивным полиномам: ($x^{19}+x^{18}+x^{17}+x^{14}+1$; $x^{22}+x^{21}+1$; $x^{23}+x^{22}+x^{21}+x^{8}+1$).

Темным цветом выделены биты, от которых существенно зависят функции обратной связи. Все три регистра используют псевдослучайное тактирование, которое работает по следующему правилу: биты с отвода 8 первого ЛРР, а также с отводов 10 второго и третьего ЛРР, подаются на так называемый *мажоритарный элемент*. Последний выдает на выходе значение 0 или 1, в зависимости от того, появляется ли на его входах больше нулей или единиц. Далее выход этого мажоритарного элемента сравнивается со значениями выходов на трех отводах ЛРР с номерами 8, 10, 10 (которые подавались ранее на входы этого мажоритарного элемента), и каждый ЛРР продвигается на один такт тогда и только тогда, когда сравниваемые биты оказываются одинаковыми. Шифрующая гамма формируется как сумма по модулю 2 выходов всех трех ЛРР. Ключом являются начальные заполнения всех ЛРР, которые вводятся на начальном этапе без псевдослучайного тактирования. Общая длинна ключа составляет 64 бита. [3]

ИССЛЕДОВАНИЕ НАДЕЖНОСТИ ШИФРА A5/1

Проведем небольшое исследование шифра A5/1 на предмет анализа стойкости и проверим возможности её повышения.

Тестировать полученную последовательность будем с помощью статического теста для генераторов случайных чисел FIPS 140 - 1 и FIPS 140 – 2.

Рассматриваемый стандарт FIPS 140 – 1 рекомендуется для оперативного тестирования последовательностей, формируемых некоторым ГПСП (генератором псевдослучайных последовательностей) и использует 4 теста. При этом для проведения тестирования требуется битовая строка длиной 20 тыс. бит. При этой длине исследуемой последовательности допустимые интервалы для статистик, вычисляемых по каждому из тестов, задаются в явном виде (то есть нет необходимости предварительно выбирать соответствующие уровни значимости).

В стандарте FIPS 140 – 2 для уменьшения вероятности принятия ошибочного решения были пересмотрены (сделаны более жесткими) допустимые интервалы для каждого из статистических тестов.

Рассмотрим кратко предлагаемые стандартом тесты [6]:

1. Монобитный тест (частотный тест).

В исследуемой последовательности количество единичных бит N_1 должно находиться в следующем интервале:

FIPS 140 -1 $9654 < N_1 < 10346$

FIPS 140 -2 $9725 < N_1 < 10275$

2. Покер – тест (блочный тест).

По исследуемой последовательности подсчитывается следующая статистика:

$$X_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k \qquad (1)$$

где m – длина подсчитываемых неперекрывающихся подпоследовательностей для данного стандарта (принято m=4);

n_i – количество появлений подпоследовательности i – того типа длины m (для m = 4 существует $2^m = 2^4 = 16$ типов подпоследовательностей);

k – общее количество неперекрывающихся подпоследовательностей длины m (для данного стандарта k = 20000 / 4 = 5000).

Значение полученной статистики X_3 должно находиться в следующем интервале.

FIPS 140 -1 $1.03 < X_3 < 57.4$

FIPS 140 -2 $1.16 < X_3 < 46.17$

3. Тест серий.

Серией считают подпоследовательность исходной последовательности, которая состоит из битов одного типа (либо "0", либо "1"), которым не предшествует и за которыми не следует бит того же типа ("0" или "1" соответственно).

В данном тесте для исследуемой последовательности подсчитывается количество единичных S_i и количество нулевых Z_i серий длины i (**$1 \le i \le 6$**, серии большей длины в данном тесте рассматриваются как серии длины **6**).

Тест серий считается успешно пройденным, если все **12** подсчитанных значения (S_i и Z_i, **$1 \le i \le 6$**) принадлежат соответствующим интервалам, приведенным в следующей таблице.

Таблица 1

Разрешенные интервалы

Table 1

Allowed intervals

Длина серии		1	2	3	4	5	6
Допустимые диапазона	*FIPS 140 -1*	2267-2733	1079-1421	502-748	223-402	90-223	90-223
	FIPS 140 - 2	2343-2657	1135-1365	542-708	251-373	111-201	111-201

4. Тест максимальной длины серии.

Тест считается успешно пройденным, если в исследуемой последовательности не существуют серии длиной 34 (FIPS 140 - 1), 26 (FIPS 140 - 1) и более.

ЭКСПЕРИМЕНТ

Алгоритмы рассмотренных тестов были реализованы в программной среде MatLab. Если хоть один из тестовых результатов не будет удовлетворять требованиям, то тестируемая последовательность не соответствует необходимой степени защиты стандарта FIPS.

Также для моделирования процесса генерации ПСП с помощью комбинированной схемы из ЛРР использовалась программа формирования ПСП на основе комбинированной схемы из линейных регистров сдвига [2]. Программа обеспечивает выполнение следующих функций:

– формирование трех линейных рекуррентных регистров на основе произвольных полиномов не более тридцать первой степени;

– произвольный выбор номера отвода на мажоритарный элемент от каждого из регистров, а также инверсию схемы мажоритарного элемента;

– произвольное начальное битовое заполнение сформированных линейных регистров сдвига;

– выбор шага генерации результирующей псевдослучайной последовательности и ее визуальное отображение;

– визуальное отображение псевдослучайной последовательности, формируемой отдельным регистром на очередном шаге генерации.

Начнем тестирование с получения ПСП. Программа позволяет задать: примитивные полиномы до максимальной степени 31; номер отвода от ЛРР; количество выполняемых шагов (число бит получаемой ПСП) и начальное заполнение регистров. Окно программы показано на рисунке 4. Изначально поля полиномов заполнены согласно стандарту шифра A5/1.

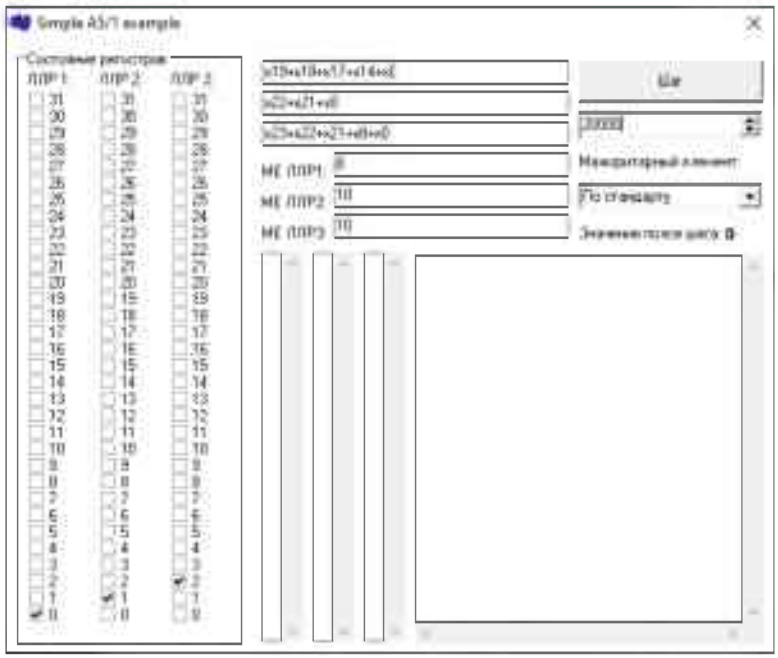

Рис. 4. Окно программы "Генератор А5-1", начальный интерфейс
Fig. 4. "Generator A5-1" program window, initial interface

После запуска программы на рисунке 5, можно увидеть сгенерированную последовательность.

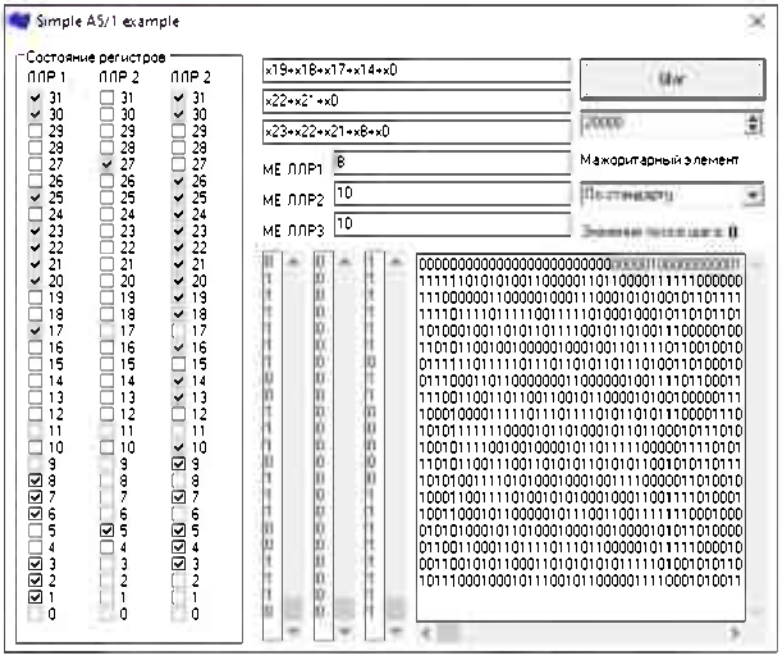

Рис. 5. Окно программы "Генератор А5-1", вывод данных
Fig. 5. Program window "Generator A5-1", data output

Полученную последовательность тестируем по стандартам FIPS 140 – 1 и FIPS 140 – 2, и получаем следующие результаты:

Таблица 2

Результат монобитного и покер теста

Table 2

The result for monobit and poker

Тесты	X	FIPS 140 – 1	FIPS 140 – 2
Монобитный	9929	9654 < X<10346	9725< X < 10275
Покер	12.25	1.03 <X<57.4	2.16 < X < 46.17

Таблица 3

Результат теста серий

Table 3

Series Test result

Серии	X_0	X_1	FIPS 140 – 1	FIPS 140 – 2
1	2629	2522	$2267<X_{0,1}<2733$	$2343 <X_{0,1}<2657$
2	1237	1197	$1079<X_{0,1}<1421$	$1135 <X_{0,1}<1365$
3	597	686	$502<X_{0,1}<748$	$542 <X_{0,1}<708$
4	300	321	$223<X_{0,1}<402$	$251 <X_{0,1}< 373$
5	157	139	$90<X_{0,1}<223$	$111 <X_{0,1}<201$
6	86	77	$90<X_{0,1}<223$	$111 <X_{0,1}< 201$

Таблица 4

Результат теста максимальной длины серий

Table 4

Test result of the maximum length of the series

Тест	X	FIPS 140 – 1	FIPS 140 – 2
Максимальная серия длинны	30	34	26

По результатам тестирования можно увидеть, что формируемая последовательность не проходит тест из 6-ти серий и тест максимальной длины серий. Из этого следует, что исследуемая последовательность на выходе комбинированной схемы из ЛЛР, соответствующей генератору A5/1, не проходит тестирование.

Таким образом, можно сделать вывод, что последовательность, формируемую комбинированной схемой A5/1, нельзя считать псевдослучайной, следовательно, ее предсказуемость значительно снижает защищенность исследуемой системы сотовой связи.

ЗАКЛЮЧЕНИЕ

В данной работе был проведен анализ стойкости алгоритма поточного шифра A5/1 с помощью статистического теста FIPS 140–1 / FIPS 140–2, реализованного в программной среде MatLab, и моделирующей программы формирования ПСП на основе комбинированной схемы из линейных рекуррентных регистров.

По результатам тестирования удалось установить, что последовательность, формируемая на основе комбинированной схемы из ЛРР A5/1, не проходит тест, и, следовательно, не является псевдослучайной. Поэтому остается актуальной задача поиска полиномов для комбинированной схемы поточного шифра в технологии GSM, позволяющей формировать последовательность с необходимыми свойствами для достижения требуемого уровня защищенности голосовой связи и данных.

Список литературы

1. Защита информации в системах мобильной связи. Учебное пособие для вузов. Под ред. А.В. Заряева и С.В. Скрыля. – 2-е изд. испр. и доп. М: Горячая линия Телеком, 2015. – 171 с.

2. Буханцов А.Д., Черноморец А.А., Болгова Е.В. "Программная система формирования псевдослучайной последовательности на основе комбинированной схемы из линейных регистров сдвига" / Свидетельство о государственной регистрации программы для ЭВМ № 2015619256 от 27.08.2015.

3. Ветров Ю.В. Криптографические методы защиты информации в телекоммуникационных системах: учеб. пособие / Ю.В. Ветров, С.Б. Макаров. – СПб.: Изд-во Политехн. ун-та, 2011. – 174 с.

4. Andreas Bubla (2004). Kryptographie in Mobilfunknetze (GSM, UMTS) [Online], availed at: https://www.bubla.info/informatik/files/krypto_gsm_umts_paper.pdf (Accessed 20 April 2021)

5. Асосков А.В., Иванов М.А., Мирский А.А., Рузин А.В., Сланин А.В., Тютвин А.Н. Поточные шифры. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.

6. Попов В.И. Основы сотовой связи стандарта GSM / В.И. Попов. – М.: Эко-Трендз, 2005. – 29 с.

References

1. Zashchita informatsii v sistemakh mobilnoy svyazi. Uchebnoye posobiye dlya vuzov. Pod red. A.V. Zaryayeva i S.V. Skrylya. – 2-e izd. ispr. i dop. M: Goryachaya liniya Telekom. 2015. – 171 s.

2. Bukhantsov A.D., Chernomorets A.A., Bolgova E.V. "Programmnaya sistema formirovaniya psevdosluchaynoy posledovatelnosti na osnove kombinirovannoy skhemy iz lineynykh registrov sdviga" / Svidetelstvo o gosudarstvennoy registratsii programmy dlya EVM № 2015619256 ot 27.08.2015

3. Vetrov Yu.V. Kriptograficheskiye metody zashchity informatsii v telekommunikatsionnykh sistemakh: ucheb. posobiye / Yu.V. Vetrov. S.B. Makarov. – SPb.: Izd-vo Politekhn. un-ta. 2011. – 174 s.

4. Andreas Bubla (2004). Kryptographie in Mobilfunknetze (GSM, UMTS) [Online], availed at: https://www.bubla.info/informatik/files/krypto_gsm_umts_paper.pdf (Accessed 20 April 2021)

5. Acoskov A.V., Ivanov M.A., Mirskiy A.A., Ruzin A.V., Slanin A.V. Tyutvin A.N. Potochnyye shifry. – M.: KUDITs-OBRAZ. 2003. – 336 s.

6. Popov V.I. Osnovy sotovoy svyazi standarta GSM / V.I. Popov. – M.: Eko-Trendz. 2005. – 296 s.

Буханцов Андрей Дмитриевич, кандидат технических наук, старший научный сотрудник, доцент кафедры информационно-телекоммуникационных систем и технологий
Саджид Александр Юрьевич, студент кафедры информационно-телекоммуникационных систем и технологий
Устинов Алексей Николаевич, студент кафедры информационно-телекоммуникационных систем и технологий
Родионов Сергей Викторович, кандидат технических наук, доцент, доцент кафедры транспортной связи

Buhantsov Andrey Dmitrievich, Candidate of Technical Sciences, Senior Researcher, Associate Professor of the Department of Information and Telecommunications Systems and Technologies
Sajiid Alexander Yuryevich, student of the Department of Information and Telecommunications Systems and Technologies
Ustinov Alexey Nikolaevich, student of the Department of Information and Telecommunications Systems and Technologies
Rodionov Sergey Viktorovich, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Transport Communications