СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2018. – № 3–4 (93).** – 116–135

УДК 621. 396 DOI: 10.17212/2307-6879-2018-3-4-116-135

# ВЫБОР КЛЮЧЕЙ ШИФРОВАНИЯ ДЛЯ ГИДРОАКУСТИЧЕСКОГО КАНАЛА СВЯЗИ*

Б.И. ФИЛИППОВ[1], А.С. ЩЕДРИНА[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, доцент, кандидат технических наук. E-mail: filippov-boris@rambler.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, студент кафедры защиты информации. E-mail: miss.shedrina@mail.ru*

Наиболее подходящим алгоритмом для шифрования в гидроакустическом канале связи является шифр RC4. Он позволяет достаточно быстро шифровать и дешифровать информацию и применять ключи с переменной длиной. Но даже этот алгоритм нуждается в доработках. Главная проблема – генерирование эффективных ключей. Они обычно формируются генераторами псевдослучайных последовательностей (ПСП), и важно, чтобы эти генераторы генерировали «чисто» случайные последовательности для наибольшей стойкости шифра. Кроме того, нужно учитывать, что может возникнуть потребность менять размеры ключей в диапазоне от 5 до 64 байт в зависимости от расстояния между объектами и скорости их движения, что позволит выбирать ключ либо большей, либо меньшей длины. Второе – это необходимость синхронизации при передаче и приеме сообщений, поэтому обязательна жесткая система синхронизации. Для получения наилучшей шифрограммы и, соответственно, обеспечивающей наивысший уровень защиты передаваемой информации был проведен сравнительный анализ схем построения генераторов ПСП. Приведенный анализ позволяет сделать вывод, что для повышения стойкости алгоритмов шифрования речи рекомендуется использовать схему Фибоначчи. Кроме того, для схемы Фибоначчи была проведена оценка степени влияния на характеристики генераторов ПСП количества порождающих полиномов. Анализ остаточной разборчивости показал, что в зашифрованном файле нельзя разобрать ни одного слова, следовательно, остаточная разборчивость равна нулю, что подтверждает эффективность предлагаемого метода защиты информации.

**Ключевые слова:** алгоритм шифрования, алгоритм дешифрования, псевдослучайная последовательность, ключи шифрования, шифрограмма, генераторы псевдослучайных последовательностей, порождающий полином, синхропосылка, криптографическая стойкость

* Статья получена 19 декабря 2018 г.

## ВВЕДЕНИЕ

Особенности гидроакустических каналов связи были рассмотрены в работах [1–11]. В частности, в [1, 2] исследовались статистические характеристики сигналов и помех, в [3, 4] – принципы построения гидроакустических систем и их энергетические характеристики, в [8, 9] рассмотрены вопросы надежности подобных систем, в [10, 11] – вопросы применения помехоустойчивого кодирования.

Данная работа посвящена вопросам криптографической защиты таких каналов. Наиболее подходящим алгоритмом для шифрования в гидроакустическом канале связи является шифр RC4 [5, 12, 13]. Он позволяет достаточно быстро шифровать и дешифровывать данные и может применяться с переменной длиной ключа. Но даже этот алгоритм нуждается в доработках. Первое, что хочется отметить, это ключ. Он обычно формируется через генератор псевдослучайных последовательностей, и важно, чтобы этот генератор выдавал «чисто» случайные последовательности для наибольшей стойкости шифра. Кроме того, необходимо учитывать, что размеры ключа могут быть в диапазоне от 5 до 64 байт, поэтому в зависимости от расстояния между объектами и скорости их движения можно выбирать ключ либо большей, либо меньшей длины. Второе – это необходимость синхронизации при передаче и приеме сообщений. То есть необходимо разработать жесткую систему синхронизации, чтобы из всех принимаемых сигналов можно было принять верный.

В данной работе рассмотрим возможные пути уменьшения влияния первой проблемы (генерация псевдослучайных последовательностей).

## 1. ПОСТАНОВКА ЗАДАЧИ И РЕШЕНИЕ

При синтезе и реализации криптографических модулей весьма важную роль играет выработка и распределение криптографически значимой информации (ключей, синхропосылок и т. п.). Важную и криптографически значимую роль играет выработка случайного числа, используемого для «индивидуализации» процесса подписи каждого сообщения.

Для решения задач создания (формирования) ключевой информации применяются различного рода генераторы псевдослучайных чисел, которые делятся на два больших класса – программные и аппаратные [13]. В аппаратных генераторах источником случайного процесса является шум в электронных приборах. Очевидно, применение аппаратных генераторов требует наличия специального оборудования. Обычно для генерации последовательности псевдослучайных чисел применяют компьютерные программы, которые на самом деле выдают детерминированные числовые последовательности, по своим свойствам похожие на случайные.

Генерируемые псевдослучайные ряды чисел часто называют гаммой шифра или просто гаммой (от буквы $\gamma$ греческого алфавита, часто используемой в математических формулах для обозначения случайных величин).

К криптографически стойкому генератору псевдослучайной последовательности чисел (гаммы шифра) предъявляются три основных требования:

- период гаммы должен быть достаточно большим для шифрования сообщений различной длины;
- гамма должна быть практически непредсказуемой, что означает невозможность предсказать следующий бит гаммы, даже если известны тип генератора и предшествующий отрезок гаммы;
- генерирование гаммы не должно вызывать больших технических сложностей.

Длина периода гаммы является наиболее значимой характеристикой генератора псевдослучайных чисел. По окончании периода числа начнут повторяться, и их можно будет предсказать. Требуемая длина периода гаммы определяется степенью закрытости данных. Чем длиннее ключ, тем труднее его подобрать. Длина периода гаммы зависит от выбранного алгоритма получения псевдослучайных чисел.

Второе требование связано со следующей проблемой: как можно достоверно убедиться, что псевдослучайная гамма конкретного генератора является действительно непредсказуемой. В настоящее время не существуют такие универсальные и практически проверяемые критерии и методики. Чтобы гамма считалась непредсказуемой, т. е. истинно случайной, необходимо, чтобы ее период был очень большим, а различные комбинации битов определенной длины были равномерно распределены по всей ее длине.

Третье требование обусловливает возможность практической реализации генератора программным или аппаратным путем с обеспечением необходимого быстродействия.

Таким образом, независимо от выбранного алгоритма необходимо выбрать генератор случайных последовательностей. Для этого рассмотрим некоторые из них.

***Линейный конгруэнтный генератор.*** Из известных процедур генерации последовательности псевдослучайных целых чисел наиболее часто применяется так называемый линейный конгруэнтный генератор. Этот генератор вырабатывает последовательность псевдослучайных чисел $Y_1$, $Y_2$, $Y_3$,..., $Y_{i-1}$, $Y_i$,..., используя соотношение

$$Y_i = (aY_{i-1} + b) \bmod m, \qquad (1)$$

где $Y_i$ – текущее число последовательности; $Y_{i-1}$ – предыдущее число последовательности; $a$, $b$ – константы; $m$ – модуль; $a$ – множитель (коэффициент); $b$ – приращение; $Y_0$ – порождающее число (исходное значение).

Уравнение (1) генерирует псевдослучайные числа с периодом повторения, который зависит от выбираемых значений параметров $a$, $b$, $m$. Если $a$, $b$, $m$ выбраны правильно, то генератор будет с максимальным периодом (например, $b$ должно быть взаимно простым с $m$, а коэффициент $a$ должен быть нечетным числом). Значение модуля $m$ берется равным $2n$ либо равным простому числу.

Преимуществом линейных конгруэнтных генераторов является их быстрота за счет малого количества операций на бит.

Конгруэнтные генераторы, работающие по алгоритму, предложенному Национальным бюро стандартов США, используются, в частности, в системах программирования [12]. Эти генераторы имеют длину периода 224 и обладают хорошими статистическими свойствами. Однако такая длина периода мала для криптографических применений. Кроме того, доказано, что последовательности, генерируемые конгруэнтными генераторами, не являются криптографически стойкими.

Однако линейные конгруэнтные генераторы сохраняют свою полезность для некриптографических приложений (например, для моделирования). Они эффективны в большинстве используемых эмпирических тестов и демонстрируют хорошие статистические характеристики.

***Линейные рекуррентные регистры.*** Существует способ генерации последовательностей псевдослучайных чисел на основе линейных рекуррентных соотношений.

Рассмотрим рекуррентные соотношения через их разностные уравнения:

$$\sum_{j=0}^{k} h_j a_{i+j} = 0,$$
$$a_{i+k} = -\sum_{j=0}^{k-1} h_j a_{i+j}, \qquad (2)$$

где $h_0 \neq 0$, $h_k = 1$, и каждое $h_i$ принадлежат полю GF(q).

Решением этих уравнений является последовательность элементов $a_0$, $a_1$, $a_2$,... поля GF(q). Соотношение (2) определяет правило вычисления $a_k$ по известным значениям величин $a_0$, $a_1$, $a_2$,..., $a_{k-1}$. По известным зна-

чениям $a_0$, $a_1$, $a_2$,..., $a_k$ находят $a_{k+1}$ и т. д. В результате по начальным значениям $a_0$, $a_1$, $a_2$,..., $a_{k-1}$ можно построить бесконечную последовательность, причем каждый ее последующий член определяется из $k$ предыдущих. Последовательности такого вида легко реализуются на компьютере, при этом реализация получается особенно простой, если все $h_i$ и $a_i$ значения 0 и 1 из поля GF(2).

На рис. 1 показана линейная последовательная переключательная схема, которая может быть использована для вычисления суммы и, следовательно, для вычисления значения $a_k$ по значениям $k$ предыдущих членов последовательности.

Исходные величины $a_0$, $a_1$, $a_2$,..., $a_{k-1}$ помещаются в разряды сдвигового регистра, последовательные сдвиги содержимого которого соответствуют вычислению последовательных символов, при этом выход после $i$-го сдвига равен $a_i$. Данное устройство называют генератором последовательности чисел, построенным на базе линейного сдвигового регистра с обратной связью (linear feedback shift register, LFSR).

Как правило, в реальных криптосхемах линейный регистр сдвига с обратной связью (рис. 1) реализуется в одной из двух различных конструкций, именуемых, соответственно, регистрами Фибоначчи или Галуа. Все наиболее важные теоретические результаты справедливы для обоих типов [14].

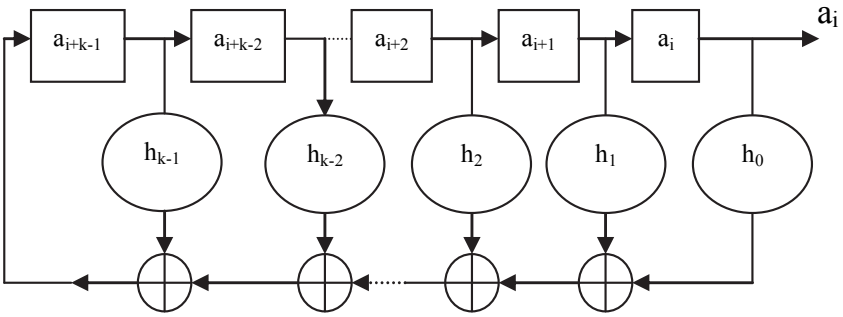



*Рис. 1.* Генератор с регистром сдвига

***Регистры Фибоначчи.*** В литературе значительно чаще обращаются к регистрам Фибоначчи. Функция обратной связи здесь – простое сложение операций XOR (исключающее или) определенных битов регистра. Перечень этих битов называется отводной последовательностью. Схема регистра Фибоначчи показана на рис. 2.

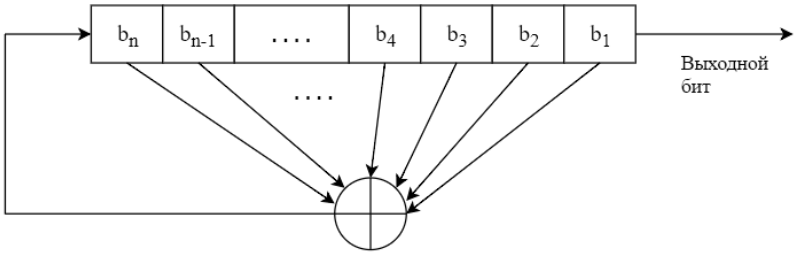



*Рис. 2.* Регистр Фибоначчи

*N*-битовый LFSR может находиться в одном из $(2^n - 1)$ внутренних состояний. Это означает, что теоретически такой регистр может генерировать псевдослучайную последовательность с периодом $(2^n - 1)$ битов. Только при определенных отводных последовательностях LFSR циклически пройдет через все $(2^n - 1)$ внутренних состояний. Такие LFSR являются LFSR с максимальным периодом. Для того чтобы LFSR имел максимальный период, многочлен, образованный от отводной последовательности и константы 1, должен быть примитивен по модулю 2. Степень многочлена является длиной сдвигового регистра. Примитивный многочлен степени $n$ – это неприводимый многочлен, который является делителем $(x^{2^{n-1}} + 1)$, но не является делителем $x^d + 1$ для всех $d$, являющихся делителями $(2^n - 1)$.

В общем случае не существует простого способа генерировать примитивные многочлены данной степени по модулю 2. Проще всего выбирать многочлен случайным образом и проверять, не является ли он примитивным.

Примеры некоторых примитивных полиномов приведены в таблице.

**Примитивные полиномы**

| Длина периода | Многочлен |
|---|---|
| 22 – 1 | (2, 1, 0) |
| 23 – 1 | (3, 1, 0) |
| 24 – 1 | (4, 1, 0) |
| 25 – 1 | (5, 2, 0) |
| 26 – 1 | (6, 1, 0) |
| 27 – 1 | (7, 1, 0) |
| 28 – 1 | (8, 6, 5, 1, 0) |

Окончание таблицы

| Длина периода | Многочлен |
|---|---|
| 211 – 1 | (11, 2, 0) |
| 212 – 1 | (12, 7, 4, 3, 0) |
| 213 – 1 | (13, 4, 3, 1, 0) |
| 214 – 1 | (14,12, 11, 1, 0) |
| 216 – 1 | (16, 5, 3,2, 0) |
| 218 – 1 | (18, 7, 0) |
| 220 – 1 | (20, 3, 0) |
| 221 – 1 | (21, 2, 0) |
| 222 – 1 | (22, 1, 0) |
| 223 – 1 | (23, 5, 0) |
| 224 – 1 | (24, 4, 3, 1, 0) |
| 225 – 1 | (25, 3, 0) |
| 227 – 1 | (27, 8, 7, 1, 0) |
| 230 – 1 | (30, 16, 15, 1, 0) |
| 231 – 1 | (31, 3, 0) |
| 232 – 1 | (32, 7, 6, 2, 0) |

Например, запись (14, 12, 11, 1, 0) означает, что следующий многочлен примитивен по модулю 2: $x^{14} + x^{12} + x^{11} + x + 1$.

Первым числом является длина LFSR. Последнее число всегда равно нулю, и его можно опустить. Все числа, за исключением 0, задают отводную последовательность, отсчитываемую от левого края регистра. Далее запись (14, 12, 11, 1, 0) означает, что для взятого 32-битового регистра сдвига новый бит генерируется с помощью XOR четырнадцатого, двенадцатого, одиннадцатого и первого битов и результирующая последовательность будет иметь максимальный период – она пройдет через $(2^{14} - 1)$ значений до того, как начнет повторяться.

Следует отметить, что все полиномы обратной связи, приведенные в таблице, являются прореженными, то есть имеют лишь несколько ненулевых коэффициентов. Прореженность – это всегда источник слабости, облегчающей вскрытие такого алгоритма генерации. Для криптографических алгоритмов лучше использовать плотные примитивные многочлены, генерировать которые по модулю 2 нелегко. В общем случае для генерации примитивных многочленов степени $k$ нужно знать разложение на множители числа $(2^k - 1)$.

***Регистры Галуа.*** Схему обратной связи LFSR можно модифицировать. Получающийся генератор не будет криптографически более надежным, но он всё еще будет обладать максимальным периодом, и его легче реализовать программно.

Вместо использования для генерации нового крайнего левого бита отводной последовательности выполняется XOR каждого бита отводной последовательности с выходом генератора и замена его результатом действия, затем результат генератора становится новым крайним левым битом. Схема регистра Галуа показана на рис. 3.

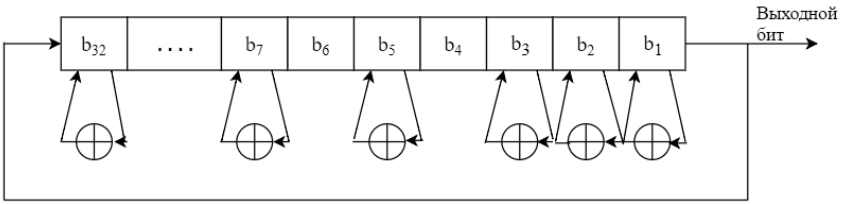



*Рис. 3.* Регистр Галуа

Таким образом, в отличие от регистра Фибоначчи, где обратная связь является функцией от всех ячеек в регистре, а результат помещается в самую левую ячейку, обратная связь в регистре Галуа потенциально применима к каждой ячейке регистра, хотя является функцией только от самой правой ячейки [15]. Выигрыш здесь в том, что все операции XOR можно выполнять как одну операцию.

Подводя общий итог, можно сказать, что если используется элементная база с быстрой реализацией сдвигов, то следует обратиться к регистрам Фибоначчи; если же есть возможность применить распараллеливание, то лучший выбор – регистр Галуа.

Но как бы хорошо не был подобран полином обратной связи, регистр сдвига с обратной связью (LFSR) остается линейным устройством. А такие устройства обычно легко поддаются криптоанализу независимо от того, насколько много параметров сохраняется в тайне. В современной криптографической литературе регистры сдвига с линейной обратной связью, как и линейные конгруэнтные генераторы, сами по себе не рекомендуются в качестве генераторов псевдослучайных шифрующих последовательностей. В то же время подавляющее большинство реальных конструкций для поточного шифрования (гаммирования) строится на основе LFSR.

Использование LFSR в программной реализации криптосхем намного проблематичней. Эффективны по скорости лишь прореженные полиномы, но

они слабы в отношении корреляционных атак; плотные же полиномы обратной связи слишком неэффективны. Стандартный поточный шифр выдает по одному биту за раз, и этот алгоритм приходится итерировать 64 раза для шифрования, а DES это делает за одну итерацию. Фактически оказывается, что несложный LFSR-алгоритм типа сжимающего генератора в программной реализации оказывается не быстрее, чем значительно более сложный DES.

***Генератор Геффа.*** В этом генераторе потока ключей используются три LFSR, объединенные нелинейным образом. Два LFSR являются входами мультиплексора, а третий LFSR управляет выходом мультиплексора. Схема генератора Геффа показана на рис. 4. Если $a_1$, $a_2$, $a_3$ – выходы трех LFSR, выход генератора Геффа можно описать выражением [14]:

$$b = \left(a_1^{a_2}\right) + (-a)^{a_3}. \tag{3}$$

Если длины LFSR равны $n_1$, $n_2$, $n_3$ соответственно, то линейная сложность генератора равна [6]:

$$(n_1 + 1)n_2 + n_1 n_3. \tag{4}$$

Период генератора равен наименьшему общему делителю периодов трех генераторов. При условии, что степени трех примитивных многочленов обратной связи взаимно просты, период этого генератора будет равен произведению периодов трех LFSR.

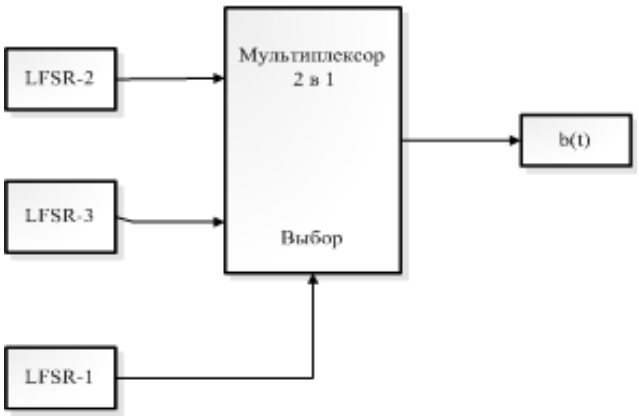



*Рис. 4.* Генератор Геффа

Хотя этот генератор неплохо выглядит на бумаге, он криптографически слаб и не может устоять против корреляционного вскрытия. В 75 % времени выход генератора равен выходу LFSR-2. Поэтому если известны отводные последовательности обратной связи, можно догадаться о начальном значении LFSR-2 и сгенерировать выходную последовательность этого регистра. Тогда можно подсчитать, сколько раз выход LFSR совпадает с выходом генератора. Если начальное значение определено неверно, две последовательности будут согласовываться в 50 % времени, а если правильно, то в 75 % времени.

Аналогично, выход генератора равен выходу LFSR в 75 % отсчетов времени. С такими корреляциями генератор потока ключей может быть легко взломан.

## 2. РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНЫХ ИСПЫТАНИЙ

Для построения генератора ПСП, позволяющего получить наилучшую шифрограмму и, соответственно, наивысший уровень защиты передаваемой речи, был проведен сравнительный анализ схем построения генераторов ПСП [16]. Как было описано выше, на сегодняшний день применяются две схемы построения: схема Галуа и схема Фибоначчи. Результаты тестирования характеристик каждой из схем для одинаковых исходных порождающих полиномов генератора Геффа приведены ниже.

Для проверки частот встречаемости символов были оценены длины серий «1» и «0», частота биграмм и триграмм. Результаты исследования параметров генератора Геффа на основе схемы Фибоначчи приведены на рис. 5–7.

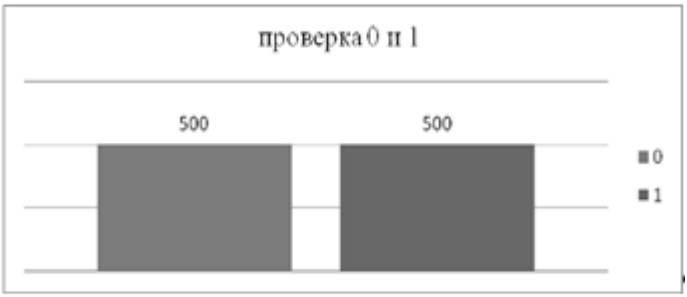



*Рис. 5.* Проверка серий для генератора Геффа (схема Фибоначчи)

Те же самые тесты были проведены для регистра Галуа [16], результаты испытаний показаны на рис. 8–10.

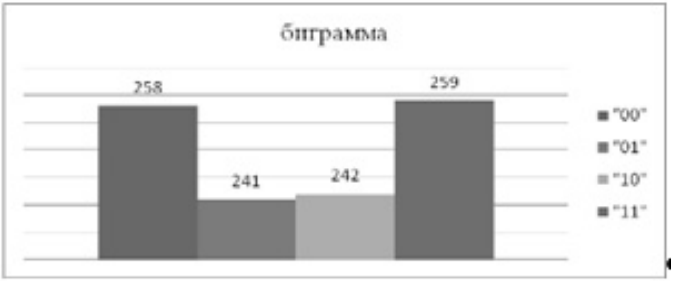



*Рис. 6.* Частота встречаемости биграмм для генератора Геффа (схема Фибоначчи)

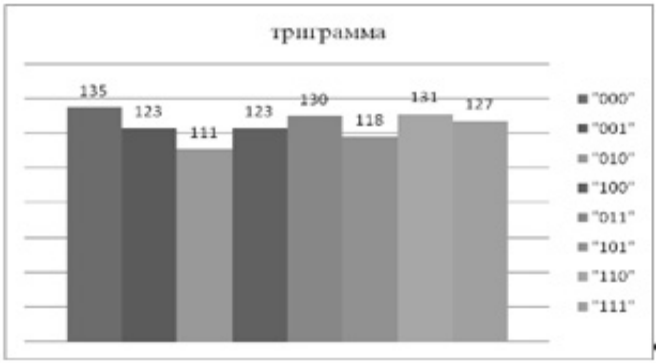



*Рис. 7.* Частота встречаемости триграмм для генератора Геффа (схема Фибоначчи)

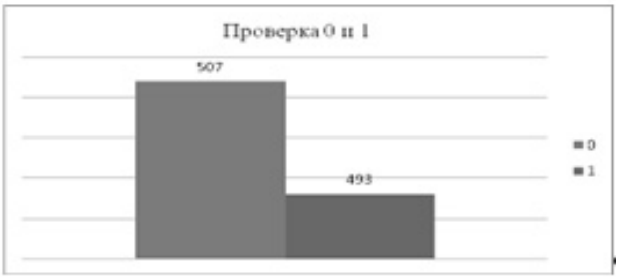



*Рис. 8.* Проверка серий для генератора Геффа (схема Галуа)

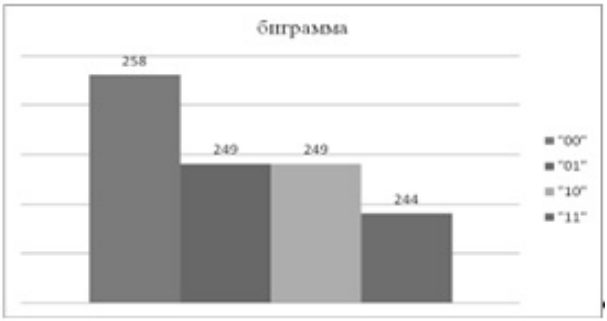



*Рис. 9.* Частота встречаемости биграмм для генератора Геффа (схема Галуа)

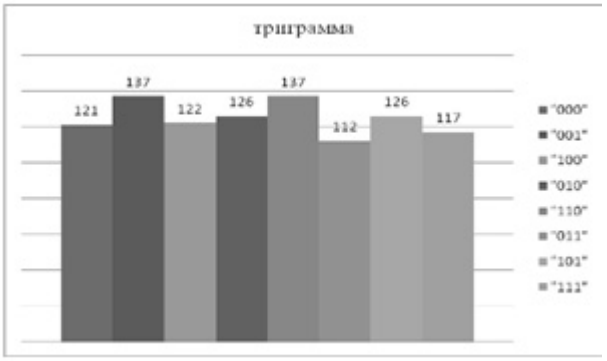



*Рис. 10.* Частота встречаемости триграмм для генератора Геффа (схема Галуа)

По полученным результатам можно сделать следующие выводы.

1. Сравнение частоты встречаемости символов (проверка серий) показывает значительное преимущество схемы Фибоначчи, у которой выборка с длиной периода в 1000 символов состоит поровну из «1» и «0», в то время как у схемы Галуа имеет место значительный перекос в сторону нулевых элементов.

2. Сравнительный анализ биграмм позволяет отдать незначительное преимущество схеме построения Галуа. Поскольку преимуществом схемы Фибоначчи является совпадение частоты встречаемости двух пар биграмм, имеет место больший разброс относительно среднего значения и, следовательно, высокая частота встречаемости одной из биграмм. В схеме Галуа пара

биграмм имеет одинаковую частоту встречаемости, а оставшиеся биграммы имеют небольшие отклонения от центральной частоты.

3. Анализ триграмм не позволяет отдать преимущество ни одной из схем, поскольку в обеих схемах разница между максимальным и минимальным значениями частоты встречаемости практически одинакова.

Приведенный анализ позволяет сделать вывод, что для повышения стойкости алгоритмов шифрования речи рекомендуется использовать схему Фибоначчи.

Кроме того, для схемы Фибоначчи была проведена оценка степени влияния на характеристики генераторов ПСП количества порождающих полиномов.

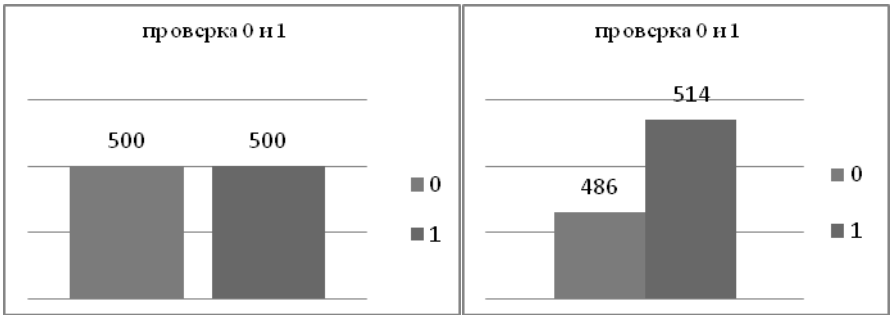
Для этого в схеме генератора Геффа в качестве порождающего во всех трех регистрах использовался в первом случае один полином вида

$$x^{24} + x^4 + x^3 + x + 1, \tag{5}$$

а во втором случае – три различных полинома вида

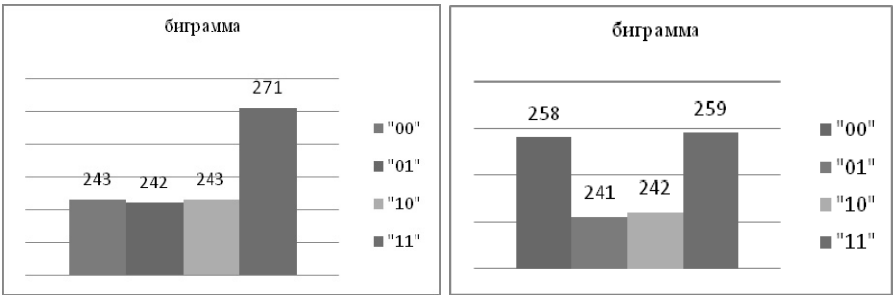
$$\begin{aligned} &x^{19} + x^{18} + x^{17} + x^{14} + 1, \\ &x^{22} + x^{21} + 1, \\ &x^{23} + x^{22} + x^{18} + x^7 + 1. \end{aligned} \tag{6}$$

Результаты исследований приведены на рис. 11–13.



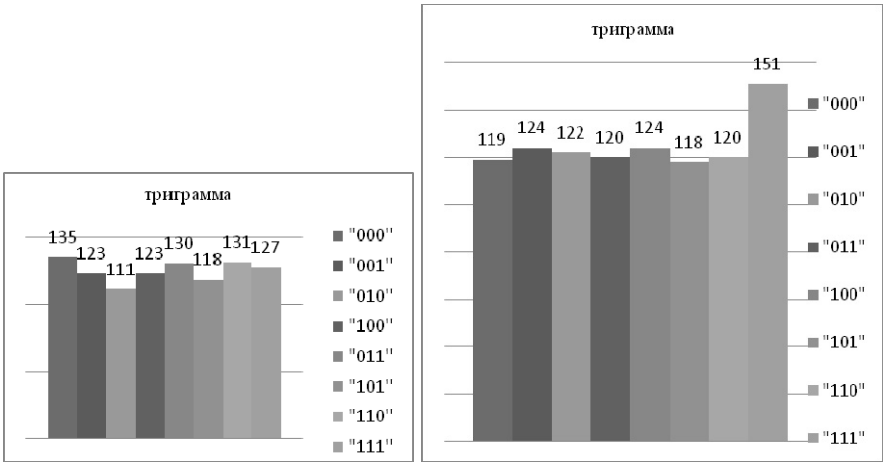

*а* *б*

*Рис. 11.* Результаты проверки серий для генератора Геффа, собранного с использованием одного (*а*) и трех порождающих (*б*) полиномов




*а* *б*

*Рис. 12.* Анализ частот встречаемости биграмм для генератора Геффа, собранного с использованием одного (*а*) и трех порождающих (*б*) полиномов




*а* *б*

*Рис. 13.* Анализ частот встречаемости триграмм для генератора Геффа, собранного с использованием одного (*а*) и трех порождающих (*б*) полиномов

Результаты исследований показывают, что значительно лучшие характеристики ПСП обеспечивает использование одного регистра. Однако полученные результаты не могут полностью считаться объективными, поскольку полученные значения зависят от типа используемого генератора и степени используемых полиномов.

Для предлагаемой схемы защиты речи необходим анализ уровня защиты. Для этого была проанализирована остаточная разборчивость речевого фраг-

мента (отношение количества слов, которые могут правильно восприняты после шифрования к общему числу переданных слов), дешифрованного при помощи генератора Геффа на основе регистров Фибоначчи. Выбор данного генератора обусловливается приведенным выше сравнительным анализом схем включения и количества генераторов.

Для анализа защищенности речевой файл был просуммирован по модулю 2 с ПСП.

Результаты испытаний приведены на рис. 14 и 15.

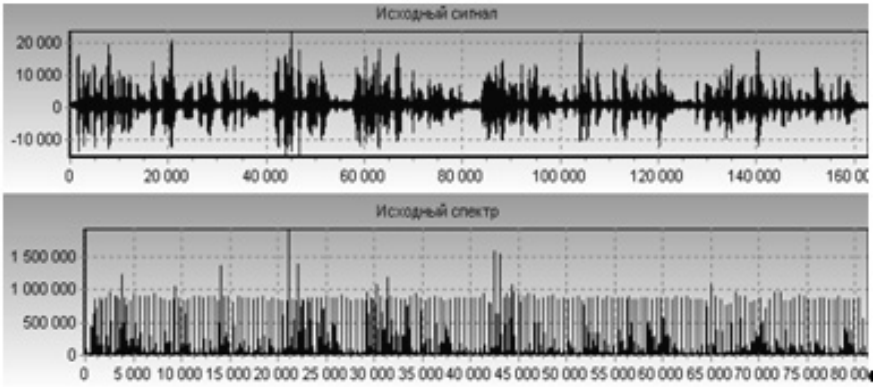



*Рис. 14.* Исходный речевой файл и его спектр

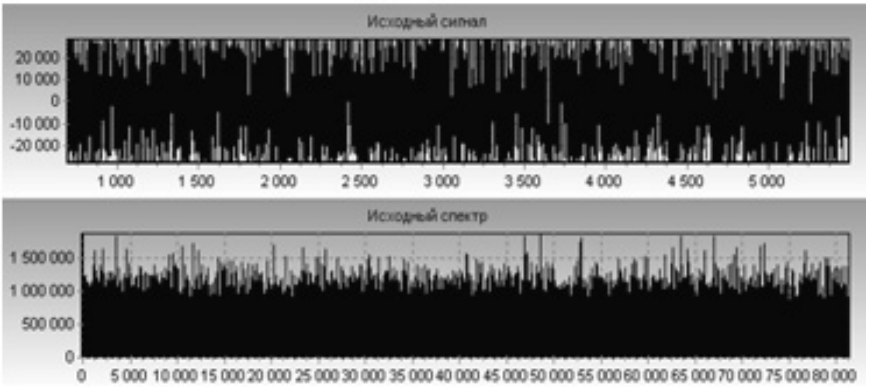



*Рис. 15.* Зашифрованный речевой файл и его спектр

Как видно из приведенных рисунков, зашифрованный файл претерпел значительные изменения. На рис. 15 мы можем наблюдать, что невозможно разобрать ни одного слова, следовательно, остаточная разборчивость равна нулю. Это подтверждает эффективность предлагаемого метода защиты информации.

## ЗАКЛЮЧЕНИЕ

Для получения наилучшей шифрограммы и, соответственно, обеспечивающей наивысший уровень защиты передаваемой информации был проведен сравнительный анализ схем построения генераторов ПСП. Приведенный анализ позволяет сделать вывод, что для повышения стойкости алгоритмов шифрования речи рекомендуется использовать схему Фибоначчи.

Кроме того, для схемы Фибоначчи была проведена оценка степени влияния на характеристики генераторов ПСП количества порождающих полиномов. Анализ остаточной разборчивости показал, что в зашифрованном файле нельзя разобрать ни одного слова, следовательно, остаточная разборчивость равна нулю, что подтверждает эффективность предлагаемого метода защиты информации.

## СПИСОК ЛИТЕРАТУРЫ

1. *Филиппов Б.И., Чернецкий Г.А.* Анализ статистических характеристик сигналов и помех в гидроакустических каналах связи // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2015. – № 3. – С. 78–84.

2. Experimental estimation of delivery success of navigation data packages transmitted via digital hydroacoustic communication channel / K.G. Kekal, V.K. Kebkal, A.G. Kebkal, R. Petroccia // Gyroscopy and Navigation. – 2016. – Vol. 7, N 4. – P. 343–352.

3. *Филиппов Б.И., Малахова Е.А.* Принципы построения систем гидроакустической связи // Вестник РГРТУ. – 2017. – № 62. – С. 33–40.

4. *Филиппов Б.И.* Энергетический расчет гидроакустических линий связи // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2016. – № 3. – С. 81–91.

5. *Басалова Г.В.* Основы криптографии. – 2-е изд. – М.: Интуит, 2016. – 283 с.

6. *Филиппов Б.И., Чернецкий Г.А.* Выбор ансамбля сигналов для передачи команд управления в гидроакустических каналах связи // Известия ВолгГТУ. – 2015. – № 3 (161). – С. 69–72.

7. *Филиппов Б.И.* Выбор метода разделения сигналов в гидроакустическом канале управления // Вестник РГРТУ. – 2018. – № 66, ч. 1. – С. 29–34.

8. *Филиппов Б.И., Малахова Е.А.* Расчет надежности донной части аппаратуры гидроакустического канала связи // Сборник научных трудов НГТУ. – 2015. – № 3 (81). – С. 79–97.

9. *Филиппов Б.И., Малахова Е.А.* Расчет надежности аппаратуры гидроакустического канала связи // Сборник научных трудов НГТУ. – 2015. – № 4 (82). – С. 67–91.

10. *Филиппов Б.И., Чернецкий Г.А.* Повышение достоверности передачи блоков цифровой информации по гидроакустическому каналу связи // Журнал Сибирского федерального университета. Техника и технологии. – 2016. – № 9. – С. 490–498.

11. *Филиппов Б.И.* Исследование и разработка устройства защиты от ошибок для системы передачи изображений по гидроакустическому каналу связи // Информационные технологии. – 2017. – Т. 23, № 12. – С. 897–904.

12. *Жданов О.Н.* Методика выбора ключевой информации для алгоритма блочного шифрования. – М.: Инфра-М, 2018. – 89 с.

13. *Ковтун В.Ю.* Генераторы случайных и псевдослучайных последовательностей. Статистические тесты. Криптографически безопасные генераторы псевдослучайных последовательностей [Электронный ресурс] / NRJETIX Ltd. – 2000–2008. – 16 с. – URL: www.nrjetix.com/fileadmin/doc/publications/Lectures_security/Lecture2.pdf (дата обращения: 18.03.2019).

14. *Бабенко Л.К., Ищукова Е.А.* Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов. – М.: Юрайт, 2018. – 220 с. – (Университеты России). – ISBN 978-5-9916-9244-1.

15. Поточные шифры: результаты зарубежной открытой криптологии. – М., 1997. – С. 32–33.

16. *Шнайер Б.* Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке СИ / пер.: Н. Дубнова. – 2-е изд. – М.: Диалектика, 2003. – 610 с. – ISBN 5-89392-055-4.

***Филиппов Борис Иванович***, доцент, кандидат технических наук, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – теория надежности, радиотехника и связь. Опубликовано 47 статей, два учебных пособия, учебник и монография. E-mail: filippov-boris@rambler.ru

***Щедрина Анастасия Сергеевна***, студент кафедры защиты информации Новосибирского государственного технического университета. E-mail: miss.shedrina@mail.ru

DOI: 10.17212/2307-6879-2018-3-4-116-135

## The selection of encryption keys for hydroacoustic communication channel*

**B.I. Filippov[1], A.S. Shchedrina[2]**

[1] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, the associate professor, PhD in Engineering sciences. E-mail: filippov-boris@rambler*

[2] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, the undergraduate student of Department Information Security. E-mail: miss.shedrina@mail.ru*

The most suitable algorithm for encryption in the hydroacoustic communication channel is the RC4 cipher. It allows to encrypt and decrypt information quickly and use keys with variable length. But even this algorithm needs to be improved. The main problem is the generation of efficient keys. They are usually formed by pseudo-random sequence generators (PRS) and it is important that these generators generate "pure" random sequences for the highest cipher strength. In addition, it should be noted that it may be necessary to change the size of the keys from 5 to 64 bytes, in depend of the distance between objects and the speed of their movement, and that will make it possibleto choose a key of either greater or lesser length. The second problem is the need for synchronization of sending and receiving messages, so a strict synchronization system is needed. The purpose of this work is consideration of possible ways to solve the first problem (creation of the necessary set of effective encryption keys). In order to obtain the best encryption that provides the highest level of protection for the transmitted information, a comparative analysis of the schemes of construction of PRS generators.was carried out. The analysis leads to the conclusionthat it is recommended to use the Fibonacci scheme to increase the strength of speech encryption algorithms. In addition, an assessment of the degree of influence on the characteristics of the PRS generators of the number of generating polynomials was made for the Fibonacci scheme. The analysis of residual intelligibility showed that not a single word can be parsed in the encrypted file, therefore residual intelligibility is zero, which confirms the effectiveness of the proposed method of information security.

**Keywords:** encryption algorithm, decryption algorithm, pseudo-random sequence, encryption keys, ciphertext, pseudo-random sequence generators, generating polynomial, synchro sending, cryptographic strength

## REFERENCES

1 Filippov B.I., Chernetskii G.A. Analiz statisticheskikh kharakteristik signalov i pomekh v gidroakusticheskikh kanalakh svyazi [Analysis of statistical characteristics of signals and noises in hydroacoustic communication channels]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical Uni-*

* *Received 19 December 2018.*

*versity. Series: Management, Computer Science and Informatics*, 2015, no. 3, pp. 78–84.

2. Kekal K.G., Kebkal V.K., Kebkal A.G., Petroccia R. Experimental estimation of delivery success of navigation data packages transmitted via digital hydroacoustic communication channel. *Gyroscopy and Navigation*, 2016, vol. 7, no. 4, pp. 343–352.

3. Filippov B.I., Malahova E.A. Printsipy postroeniya sistem gidroakusticheskoi svyazi [Principles of hydroacoustic communication systems creation]. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta – Vestnik of Ryazan State Radio Engineering University*, 2017, no. 4 (62), pp. 36–43.

4. Filippov B.I. Energeticheskii raschet gidroakusticheskikh linii svyazi [Energy calculation of hydroacoustic communication lines]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2016, no. 3, pp. 81–91.

5. Basalova G.V. *Osnovy kriptografii* [Basics of cryptography]. 2nd ed. Moscow, Intuit Publ., 2016. 283 p.

6. Filippov B.I., Chernetsky G.A. Vybor ansamblya signalov dlya peredachi komand upravleniya v gidroakusticheskikh kanalakh svyazi [Choice of ensemble of signals for transfer of teams management in the hydroacoustic communication channels]. *Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta – Izvestia of Volgograd State Technical University*, 2015, no. 3 (161), pp. 69–72.

7. Filippov B.I. Vybor metoda razdeleniya signalov v gidroakusticheskom kanale upravleniya [The choice of signal separation method in hydroacoustic control channel]. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta – Vestnik of Ryazan State Radio Engineering University*, 2018, no. 4 (66), pt. 1, pp. 29–34.

8. Filippov B.I., Malahova E.A. Raschet nadezhnosti donnoi chasti apparatury gidroakusticheskogo kanala svyazi [Calculation of reliability of ground part of the equipment hydroacoustic communication channel]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2015, no. 3 (81), pp. 79–97.

9. Filippov B.I., Malahova E.A. Raschet nadezhnosti apparatury gidroakusticheskogo kanala svyazi [Calculation of reliability of the equipment hydroacoustic communication channel]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2015, no. 4 (82), pp. 67–91.

10. Filippov B.I., Chernetsky G.A. Povyshenie dostovernosti peredachi blokov tsifrovoi informatsii po gidroakusticheskomu kanalu svyazi [Increase of reliability

of transfer of blocks the digital information on the hydroacoustic communication channel]. *Zhurnal Sibirskogo federal'nogo universiteta. Tekhnika i tekhnologii – Journal of Siberian Federal University. Engineering & Technologies*, 2016, no. 9, pp. 490–498.

11. Filippov B.I. Issledovanie i razrabotka ustroistva zashchity ot oshibok dlya sistemy peredachi izobrazhenii po gidroakusticheskomu kanalu svyazi [Research and development of the device of protection against mistakes for system of transfer of images on the hydroacoustic communication channel]. *Informatsionnye tekhnologii – Information Technologies*, 2017, vol. 23, no. 12, pp. 897–904.

12. Zhdanov O.N. *Metodika vybora klyuchevoi informatsii dlya algoritma blochnogo shifrovaniya* [The method of selection of key information for a block cipher algorithm]. Moscow, Infra-M Publ., 2018. 89 p.

13. Kovtun V.Yu. *Generatory sluchainykh i psevdosluchainykh posledovatel'nostei. Statisticheskie testy. Kriptograficheski bezopasnye generatory psevdosluchainykh posledovatel'nostei* [Random and pseudorandom sequence generators. Statistical test. Cryptographically secure pseudorandom sequence generators]. NRJETIX Ltd., 2000–2008. 16 p. Available at: www.nrjetix.com/fileadmin/doc/publications/Lectures_security/Lecture2.pdf (accessed 18.03.2019).

14. Babenko L.K., Ishchukova E.A. *Kriptograficheskaya zashchita informatsii: simmetrichnoe shifrovanie* [Cryptographic protection of information: symmetric encryption]. Moscow, Yurait Publ., 2018. 220 p. ISBN 978-5-9916-9244-1.

15. *Potochnye shifry: rezul'taty zarubezhnoi otkrytoi kriptologii* [Stream cipher. The results of the open foreign cryptology]. Moscow, 1997, pp. 32–33.

16. Schneier B. *Applied cryptography: protocols, algorithms and source code in C*]. 2nd ed. New York, Wiley, 1996 (Russ. ed.: Shnaier B. *Prikladnaya kriptografiya: protokoly, algoritmy i iskhodnye teksty na yazyke Si*. 2nd ed. Moscow, Dialektika Publ., 2003. 610 p. ISBN 5-89392-055-4).

Для цитирования:

*Филиппов Б.И., Щедрина А.С.* Выбор ключей шифрования для гидроакустического канала связи // Сборник научных трудов НГТУ. – 2018. – № 3–4 (93). – С. 116–135. – DOI: 10.17212/2307-6879-2018-3-4-116-135.

For citation:

Filippov B.I., Shchedrina A.S. Vybor klyuchei shifrovaniya dlya gidroakusticheskogo kanala svyazi [The selection of encryption keys for hydroacoustic communication channel]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2018, no. 3–4 (93), pp. 116–135. DOI: 10.17212/2307-6879-2018-3-4-116-135.