УДК 004.056.5

АНАЛИЗ МЕТОДОВ СКРЕМБЛИРОВАНИЯ

Мешальникова А.А.
Студент,
ФГАОУ ВО «Севастопольский государственный университет»,
Севастополь, Россия

Мирянова А.Д.
Студент,
ФГАОУ ВО «Севастопольский государственный университет»,
Севастополь, Россия

Мирянова В.Н.
Кандидат технических наук, доцент
ФГАОУ ВО «Севастопольский государственный университет»,
Севастополь, Россия

Аннотация

В настоящее время понятие информационной безопасности весьма актуально. В данной статье дается оценка существующих методов скремблирования как одного из способов защиты, например, речевого сигнала. Скремблирование применимо, если возникает необходимость зашифровать трафик, не прибегая к ресурсоёмким методам, и не требуется высокая криптостойкость; а также если необходимо уменьшить уровень излучаемых помех в системе связи, повысить надежность синхронизации устройств. Существуют цифровые и аналоговые способы закрытия речи. В статье приводится сравнительный анализ аналоговых методов скремблирования.

Ключевые слова: информационная безопасность, дешифрование, защита информации, системы связи, скремблер, скремблирование, шифрование.

ANALYSIS OF SCRAMBLING METHODS

Meshalnikova A.A.

student,

Sevastopol State University,

Sevastopol, Russia

Mirianova A.D.

student,

Sevastopol State University,

Sevastopol, Russia

Mirianova V.N.

Ph.D , Associate Professor,

Sevastopol State University,

Sevastopol, Russia

Abstract

Currently, the concept of information security is very relevant. This article evaluates the existing scrambling methods as one of the ways to protect, for example, a speech signal. Scrambling is applicable if there is a need to encrypt traffic without resorting to resource-intensive methods, and high cryptographic strength is not required; and also, if it is necessary to reduce the level of radiated interference in the communication system, to increase the reliability of device synchronization. There are digital and analog ways to close speech. The article provides a comparative analysis of analog methods of scrambling.

Keywords: information security, decryption, information protection, communication systems, scrambler, scrambling, encryption.

Введение

Аналоговое скремблирование представляет собой преобразование

речевого сигнала с его последующим восстановлением. Преобразованный сигнал искажается так, что уменьшается разборчивость.

Особенностью аналогового скремблирования является то, что обратное преобразование в исходящий сигнал не позволяет точно восстановить исходный сигнал без искажений.

Преимуществом аналогового скремблирования перед цифровым есть меньшая стоимость и сложность устройств. Кроме того, этот метод закрытия речи позволяет передавать преобразованный сигнал по телефонным каналам связи.

Методы аналогового скремблирования условно можно разделить на два типа:

а) преобразование сигнала в частотной области (инверсные и полосовые скремблеры);

б) преобразование сигнала во временной области (инверсия по времени сегментов речи и их временная перестановка).

При закрытии сообщения все перестановки отсчетов сегментов или спектральной плотности аналогового сигнала во временной и в частотной областях осуществляются по псевдослучайному закону. Псевдослучайная последовательность (ПСП), формирующая этот закон, вырабатывается генератором ключа для каждого речевого сообщения отдельно. Ключ должен быть известен разговаривающим абонентам.

1. Частотный метод закрытия речевых сообщений

Существует несколько способов частотного скремблирования. Одним из способов является инверсия спектра сигнала.

Спектральная плотность низкочастотного речевого сигнала (рис.1) переноситься в область высоких частот с помощью амплитудной модуляции косинусоидального несущего колебания с частотой f_0. Амплитудно-модулированный сигнал имеет вид

$$S_{AM}(t) = (A + S(t))\cos 2\pi f_0 t,$$

где $S(t)$ – низкочастотный речевой сигнал; A – постоянная составляющая такая, что максимальный размах $S(t)$ меньше A.

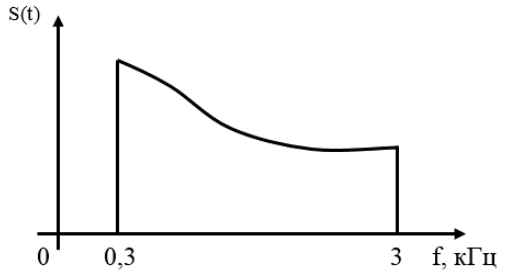


Рис. 1 – Исходный речевой сигнал [1, 4]

Сигнал с амплитудной модуляцией имеет две полосы в спектре, верхнюю и нижнюю, как показано на рис. 2. Причем, верхняя полоса по форме совпадает со смещенной на частоту f_0 модулем спектральной плотности низкочастотного сигнала и записывается как $S(\omega + \omega_0)$. В передающем устройстве верхняя полоса отфильтровывается и используется нижняя боковая полоса, которая подается в канал связи (рис. 3).

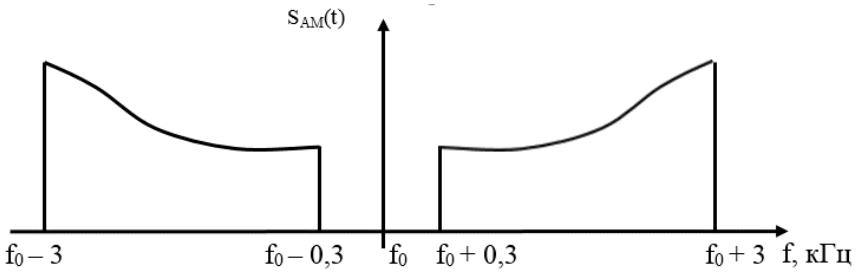


Рис. 1 – Спектр амплитудно-модулированного сигнала [4]

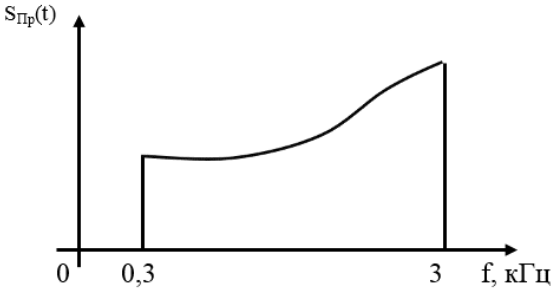
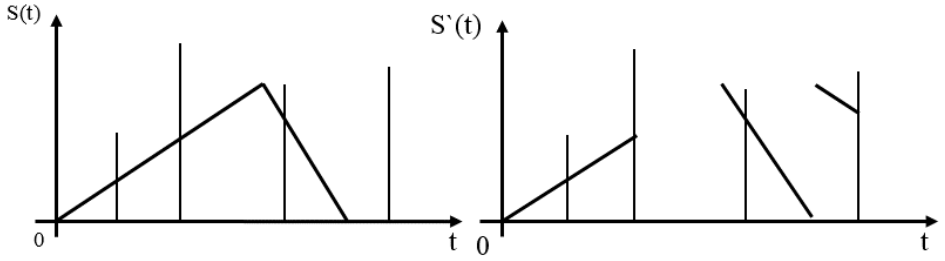


Рис. 2 – Сигнал с инвертированным спектром [1, 4]

Такое преобразование не зависит от ключа и поэтому имеет низкую степень защиты.

Большей степени защиты можно достигнуть полосно-сдвиговым инвертором, который разделяет частотный диапазон сигнала на четыре субполосы (рис. 4). Ключом выступает средняя точка полосы, которая является частотой разбиения. Ключ позволяет инвертироваться субполосе вокруг своей средней частоты.



а) б)

Рис.3 – Принцип работы полосно-сдвигового инвертора речевого сигнала: а) график исходного сигнала; б) график зашифрованного сигнала [1, 4]

Частота разбиения единственный ключевой параметр, поэтому данный метод обеспечивает невысокую степень закрытия речевого сообщения, но она больше, чем в предыдущем случае.

Третий способ преобразования сигнала в частотной области – полосовое скремблирование. Спектр сигнала делят на несколько сегментов имеющих одинаковую ширину и затем переставляют местами друг с другом и (или) инвертируют (рис. 5) [2]. Ключом является правило, на основе которого происходит перемешивание и инверсия сегментов спектра.

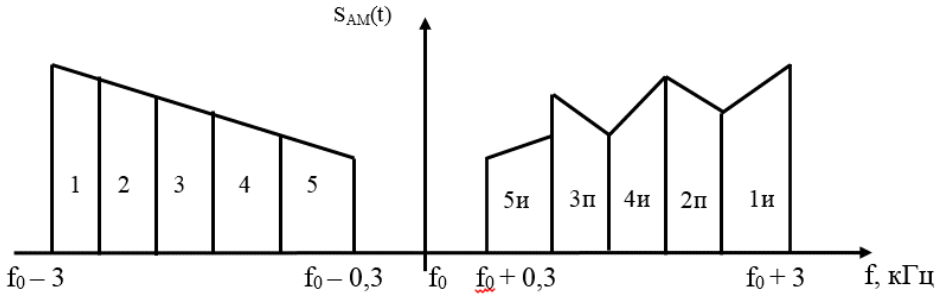


Рис. 4 – Принцип работы четырехполосного скремблера [1]

При использовании большого числа сегментов увеличивается число возможных перестановок и стойкость системы. Однако на практике это приводит к ухудшению качества восстановленного сигнала, поскольку используемые фильтры не являются идеальными.

При использовании лишь перестановок остаточная разборчивость достигает 10%, что не гарантирует стойкости закрытого сообщения. Также известно, что более 40% энергии сигнала лежит в первых двух сегментах спектра исходного сигнала, которые соответствуют первой форманте. Правильное определение положения этих сегментов в спектре преобразованного сигнала позволяет частично восстановить сигнал и разборчивость фрагмента сообщения [1].

Повысить степень закрытия речи можно реализацией быстрого преобразования Фурье (БПФ) (рис. 6) [2]. Число возможных перемешиваний частотных полос увеличится, что позволит повысить степень закрытия без снижения разборчивости речи.

Недостатком полосового скремблера с БПФ являются большие временные задержки и вычислительные затраты, связанные с необходимостью выполнять быстрое преобразование Фурье.

Рис. 5 – Основная форма реализации аналогового скремблера на основе БПФ [5]

Еще один способ заключаешься в следующем. На основе анализа основных параметров речевого сигнала делается вывод о том, что разборчивость речи можно значительно снизить, если изменить такие временные параметры как: период основного тона и длительность фонем.

Принцип получения закрытого речевого сигнала состоит в дискретизации речевого сигнала с постоянной частотой, изменении интервалов следования полученных отсчетов в соответствии с ключом и восстановлении непрерывного сигнала из измененного дискретного сигнала.

Если дискретизация осуществляется с частотой f_{const}, где $f_{\text{макс}}$ – максимальная частота в спектре сигнала. За время T будет получено $N = Tf_{const}$ отсчетов сигнала. В результате работы кодирующего устройства частота следования отсчетов принимает три различных значения: f_1, f_2 и f_3. За время T все N отсчетов сигнала должны быть переданы адресату, чтобы выполнялось равенство

$$\frac{3}{f_{const}} = \frac{1}{f_1} + \frac{1}{f_2} + \frac{1}{f_3}.$$

2. Временной метод закрытия речевых сообщений

Данный вид скремблеров основывается на разбиении речевого сигнала на кадры, которые делятся на сегменты и перемешиваются по закону ПСП (рис.7) [1].

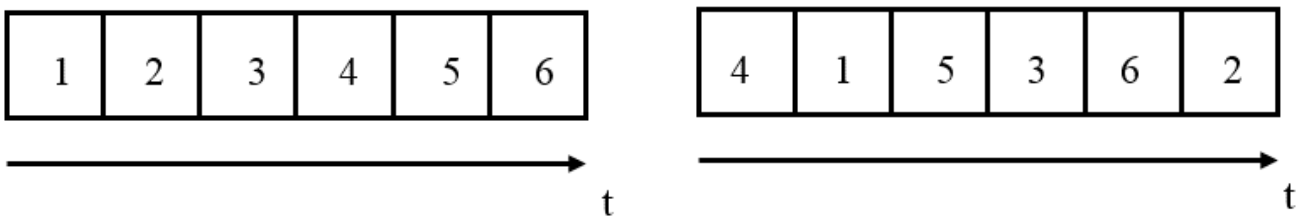


Рис. 6 – Схема работы временного скремблера с перестановками [1]

Выбор длины сегмента проверяется на практике экспериментальными проверками. Учитывается задержка, которая возникает между иходным

сигналом и восстановленым сигналом на приемнике. По сравнению с частотными скремблерами у временных скремблеров задержка значительно больше.

Также одним из ключевых параметров является перестановка. Можно взять одну фиксированную перестановку для преобразования каждого кадра. Однако, степень закрытия речи будет невысокой. Обычно используют генератор ПСП для выбора перестановок. В этом случае появляется возможность преобразовывать каждый кадр отдельно.

Недостатком скремблера, работающего с сигналом во временной области является расширение спектра сигнала, возникшее в результате перепутывания и кодирования сегментов.

Вывод

Таким образом, скремблеры, использующие лишь методы преобразования в частотной области, не могут обеспечить необходимую степень защиты. Их можно использовать лишь с целью препятствия понимания разговора или для злоумышленников, которые не обладают аналогичной аппаратурой.

Степень защиты скремблеров с временными перестановками зависит от выбора длины кадра, длины сегмента речи и правила перестановки.

Библиографический список

1. Тумбинская, М.В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М.В. Тумбинская, М.В. Петровский. — Санкт-Петербург: Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст: электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/207095.

2. Бахрушин А.П. Скремблирование цифровых изображений/ А.П. Бахрушин, Г.И. Бахрушина, Д.С. Синьков// Электронное научное издание

«Ученые заметки ТОГУ». — URL: https://pnu.edu.ru/media/ejournal/articles-2018/TGU_9_101.pdf

3. Голиков А.М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика: Учебное пособие/ А.М. Голиков.-СПб.: Издательство «Лань», 2018. –452с.

4. Кириллов, С. Н. Защита информации в МТКС : учебное пособие / С. Н. Кириллов, В. Т. Дмитриев. — Рязань : РГРТУ, 2018. — 48 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168246

5. Конахович Г. Ф. Защита информации в телекоммуникационных системах/ Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов.— К.: «МК-Пресс», 2005. — 288 с.

Оригинальность 94%