Практическая работа № 2

2 Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности

2.1 Цель практической работы.

Цель практической работы состоит в ознакомлении с методами защиты средств радиосвязи от нарушения конфиденциальности путем использования скремблирования и шифрования.

Перед выполнением практических заданий студенты должны ориентироваться в основных аспектах теоретических основ радиотехники, иметь представление о принципах функционирования средств беспроводной связи, знать принципы функционирования базовых цифровых устройств, владеть методами расчета математических выражений с использованием математических пакетов MathCad или MathLab.

В результате выполнения практического задания студенты должны освоить метод защиты средств радиосвязи от нарушения конфиденциальности путем использования средств скремблирования и шифрования.

2.2 Краткие теоретические сведения

В целях нарушения нормального функционирования ТКС могут использоваться специальные мероприятия.

Радиоэлектронная борьба (РЭБ) - это комплекс мероприятий, проводимых в целях ***разведки*** и последующего ***радиоэлектронного подавления*** радио- и оптико-электронных средств (РЭС и ОЭС) и систем инфокоммуникаций, а также радиоэлектронной защиты своих радио- и оптико-электронных средств и систем. При этом ***разведка*** беспроводных средств ТКС заключается в предварительном поиске и обнаружении радиоизлучений с последующей оценкой их параметров (частоты радиоизлучений, метода модуляции и т.п.)

Радиоэлектронное подавление (РЭП) - это мероприятия и действия соответствующих ***структур безопасности*** (подразделений или групп) по ***дезорганизации*** или ***снижению эффективности*** функционирования подавляемых радиоэлектронных средств и систем путем воздействия на них электромагнитными излучениями. Это достигается путем создания радиоэлектронных помех, применением ложных целей и ловушек, изменением электрических свойств среды, в которой распространяются электромагнитные волны, и другими способами.

Объектами РЭП являются РЭС и ОЭС локации, связи, навигации, телеуправления и другие радио- и оптико-электронные средства, составляющие *основу современных систем инфокоммуникаций.*

Сценарий РЭБ определяет следующие четыре основных требования к радиотелекоммуникационной системе (РТКС):

- Безопасность передачи сообщений с целью обеспечения невозможности раскрытия злоумышленником содержания передаваемой информации (обеспечение конфиденциальности или криптозащиты передаваемых сообщений).
- Защита каналов связи от доступа к ним злоумышленника, который может навязывать нам ложные сообщения для дезорганизации работы телекоммуникационной системы или

перехвата управления нашей технической системой. Защита каналов связи от поддельных сообщений называется имитозащитой каналов связи. В гражданских телекоммуникационных системах к этой задаче также относятся защита подписей на документах от подделок, защита электронных паролей доступа в систему, защита кредитных карточек, охранных сигнализаций и др.

- Обеспечение энергетической скрытности излучаемых радиосигналов с целью предотвратить обнаружение злоумышленником факта работы радиолинии и возможность пеленгации радиоизлучающих средств с целью их радиоэлектронного подавления.
- Защита радиолиний от радиоэлектронного подавления помехами от станций помех злоумышленников.

Обеспечение конфиденциальности (криптозащита) передаваемых сообщений

Одним из простейших способов сокрытия информации, передаваемой в цифровом (двоичном) сообщении является ***скремблирование*** двоичного сигнала этого сообщения.

Смысл скремблирования состоит в получении последовательности, в которой статистика появления нулей и единиц в информационном сигнале приближается к случайной. Это позволяет удовлетворять требованиям надежного выделения тактовой частоты и обеспечения постоянной, сосредоточенной в заданной области частот, спектральной плотности мощности передаваемого сигнала.

Скремблирование широко применяется во многих видах систем связи для улучшения статистических свойств передаваемого сигнала. При этом обычно скремблирование осуществляется непосредственно перед модуляцией несущей сигнала.

Вместе с тем, скремблирование может использоваться в качестве метода, затрудняющего несанкционированный доступ к передаваемой информации.

Скремблирование (от английского слова ***to scramble*** - перемешивать) производится на передающей стороне с помощью специального устройства - ***скремблера***, реализующего логическую операцию суммирования по модулю 2 исходного и преобразующего псевдослучайного двоичных сигналов. На приемной стороне осуществляется обратная операция - ***дескремблирование*** предварительно демодулированного сигнала устройством, называемым ***дескремблером***. ***Дескремблер*** выделяет из принятой цифровой скремблированной двоичной последовательности исходную передаваемую последовательность. Основной частью скремблера является генератор псевдослучайной последовательности (ПСП) в виде линейного ***m***-каскадного регистра сдвига с обратными связями, формирующий последовательность максимальной длины $2^{m}- 1$.

Различают два основных типа скремблеров и дескремблеров - самосинхронизирующиеся (СС) и с установкой (аддитивные).

Особенностью самосинхронизирующегося скремблера (СС-скремблера) (Рис. 2.1) является то, что он управляется скремблированной последовательностью, т.е. той, которая передается в канал связи. Поэтому при данном виде скремблирования не требуется специальной установки состояний скремблера и дескремблера: скремблированная последовательность записывается в регистры сдвига скремблера и дескремблера, устанавливая их в идентичное состояние. При потере синхронизма между скремблером и дескремблером время восстановления синхронизма не превышает числа тактов, равного числу ячеек регистра скремблера.

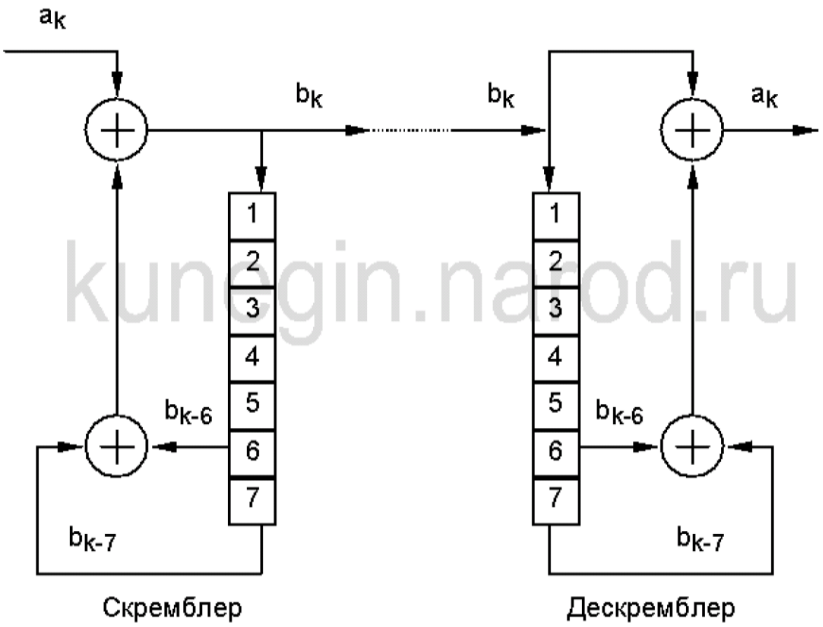

Рис. 2.1. СС-скремблер и дескремблер

На приемном конце выделение исходной последовательности происходит путем сложения по ***модулю 2*** принятой скремблированной последовательности с ПСП регистра. Например, для схемы Рис. 2.1 входная последовательность a_k с помощью скремблера в соответствии с соотношением $\mathbf{b_k=a_k \oplus (b_{k-6} \oplus b_{k-7})}$ преобразуется в посылаемую двоичную последовательность b_k. В приемнике из этой последовательности таким же регистром сдвига, как на приеме, формируется последовательность $\mathbf{a_k=b_k \oplus (b_{k-6} \oplus b_{k-7})}$. Эта последовательность на выходе дескремблера идентична первоначальной последовательности.

Как следует из принципа действия схемы, при одной ошибке в последовательности b_k ошибочными получаются также последующие шестой и седьмой символы (в данном примере). В общем случае влияние ошибочно принятого бита будет сказываться ($a+1$) раз, где a - число обратных связей. Таким образом, СС скремблер - дескремблер обладает свойством размножения ошибок. Данный недостаток СС скремблера - дескремблера ограничивает число обратных связей в регистре сдвига; практически это число не превышает $a=2$.

Второй недостаток СС скремблера связан с возможностью появления на его выходе при определенных условиях так называемых критических ситуаций, когда выходная последовательность приобретает периодический характер с периодом, меньшим длины ПСП. Чтобы предотвратить это, в скремблере и дескремблере согласно рекомендациям МСЭ-Т предусматриваются специальные дополнительные схемы контроля, которые выявляют наличие периодичности элементов на входе и нарушают ее.

Недостатки, присущие СС скремблеру - дескремблеру, практически отсутствуют при ***аддитивном скремблировании*** (Рис. 2.2), однако, здесь требуется предварительная идентичная установка состояний регистров скремблера и дескремблера.

В аддитивном скремблере с установкой (АД-скремблере), как и в СС-скремблере, производится суммирование входного сигнала и ПСП, но результирующий сигнал не поступает на вход регистра. В дескремблере скремблированный сигнал также не проходит через регистр сдвига, поэтому размножения ошибок не происходит.

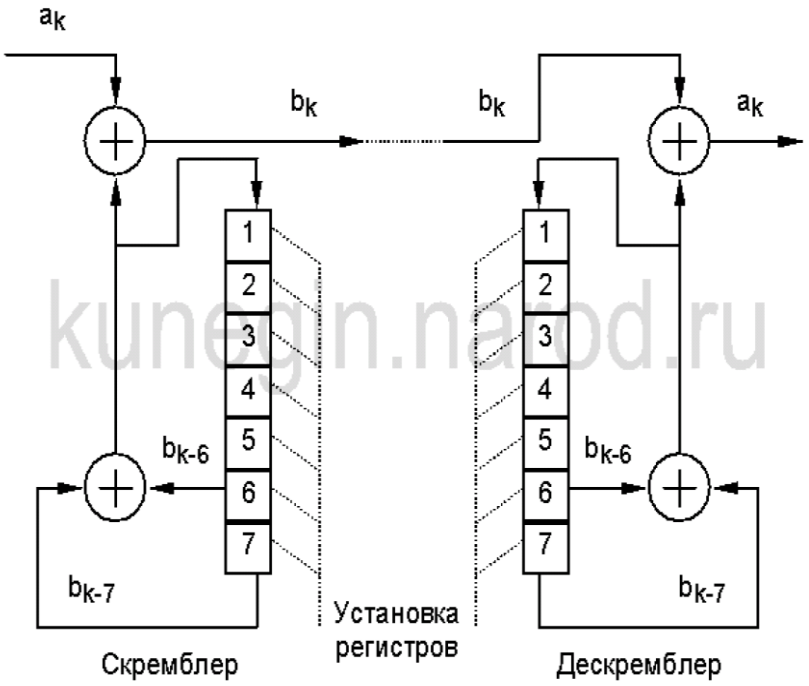

Рис. 2.2. Аддитивные скремблер и дескремблер

Суммируемые в скремблере двоичные последовательности независимы, поэтому их период всегда равен наименьшему общему кратному величин периодов входной последовательности и ПСП, поэтому критическое состояние отсутствует. Отсутствие эффекта размножения ошибок и необходимости в специальной логике защиты от нежелательных ситуаций делают способ аддитивного скремблирования предпочтительнее, если не учитывать затрат на решение задачи предварительной синхронизации (фазирования) состояний скремблера и дескремблера. В качестве сигнала установки в цифровой синхронизирующей последовательности (ЦСП) используют сигнал цикловой синхронизации.

Метод скремблирования сигнала обеспечивает недостаточно высокую стойкость скремблированного сигнала от вскрытия его параметров злоумышленниками и последующего дескремблирования передаваемого сообщения.

Поэтому в целях обеспечения более высокой степени защиты конфиденциальности передаваемой информации используются специальные криптографические методы.

В Российской Федерации установлен единый стандарт криптографического преобразования данных по ГОСТ 28147—89 при передаче информации для всех государственных органов, организаций и предприятий. Согласно этому ГОСТу режим шифрования, называемый ***режимом гаммирования***, состоит в поразрядном сложении по модулю два передаваемых двоичных сообщений с двоичной шифрпоследовательностью (гаммой), которая вырабатывается шифратором. Тактовые частоты передаваемых сообщений и шифр-последовательности одинаковы и синхронны.

Шифратор представляет собой некоторый цифровой автомат, имеющий 2^m возможных состояний. Выбор конкретного состояния шифратора производится выбором ключа. Общее число возможных ключей равно 2^m, где m называется длиной ключа, а общее число бит на периоде m – последовательности равно $N = 2^m - 1$. Для выбранного ключа шифратор преобразует входную

открытую синхропоследовательность ***S*** в шифр-последовательность ***Г*** («бегущий шифр») со свойствами абсолютно случайной двоичной последовательности.

При этом предполагается, что злоумышленник знает об используемом шифраторе все и даже физически имеет его в наличии. Единственно, что он не знает - это конкретно выбранного ключа, который оперативно должен меняться в системе шифрования. Шифратор должен быть разработан таким образом, чтобы злоумышленнику для раскрытия сообщений пришлось бы угадывать используемый ключ методом перебора всех возможных вариантов ключей, на что потребовалось бы несколько лет непрерывной работы соответствующих средств вычислительной техники.

Функциональная схема передачи сообщений с криптозащитой по линии связи представлена на рис. 2.3. Особенностью этой схемы является выбор синхропоследовательности ***S*** с большим периодом повторения (год и более), способ уплотнения ее с информационной последовательностью и способ формирования синхропоследовательности ***S*** в приемнике для различных условий передачи: непрерывная передача, пакетная передача, учет помехоустойчивого кодирования информационной последовательности и др.

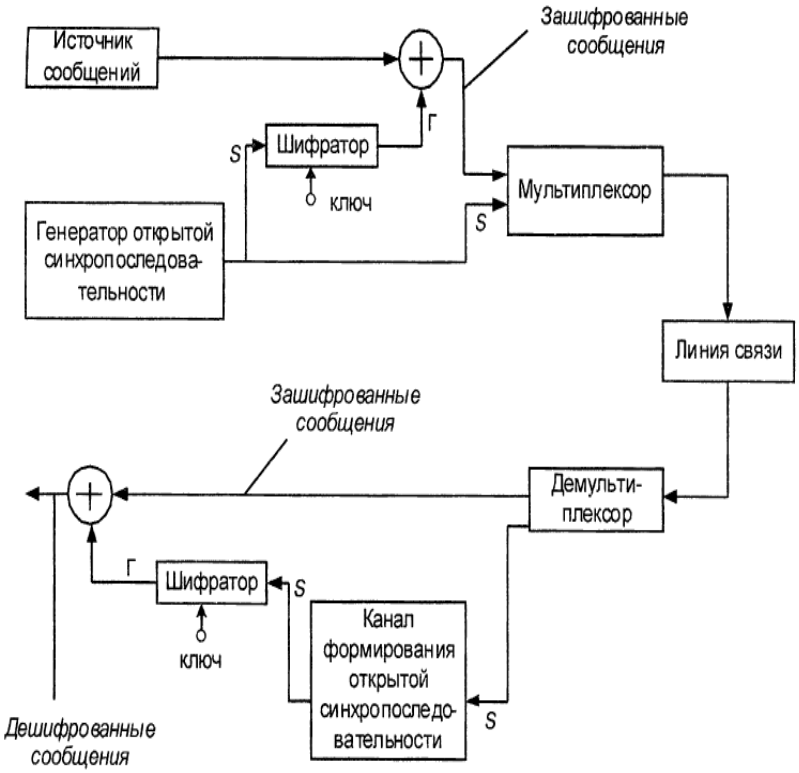

Рис. 2.3. Функциональная схема передачи сообщений с криптозащитой по линии связи

Инженерная задача заключается в организации канала передачи синхропоследовательности шифратора с помехоустойчивостью существенно выше помехоустойчивости канала информационного сообщения.

2.3. Практическое задание

1. В качестве генератора синхропоследовательности шифратора в схеме рис. 2.3 можно использовать генератор ***m***-последовательности на регистре сдвига с обратными связями.
2. Задание: определить период ***m***-последовательности, если длина регистра сдвига ***m*** = 64, а частота следования символов ***m*** - последовательности равна 2,048 Мбит/с.

2.4. Контрольные вопросы

1. Что такое РЭБ ?
2. Сколько требований и какие в связи с РЭБ предъявляются к РТКС ?
3. В чем состоит суть метода скремблирования и каково его основное назначение в ТКС?
4. Какие свойства скремблирования цифровых сообщений позволяют его использовать для повышения степени их защиты от несанкционированного доступа ?
5. Что такое скремблер и дескремблер ?
6. Что является основной частью скремблера ?
7. Сколько и какие известны основных типов скремблеров и дескремблеров ?
8. Изобразить схему СС-скремблера и дескремблера, объяснить принцип их работы и указать основные недостатки ?
9. Изобразить схему АД-скремблера и дескремблера, объяснить принцип их работы и указать основные недостатки ?
10. В чем сущность шифрования сообщения по ГОСТ 28147—89?
11. Изобразить функциональную схему передачи сообщений с криптозащитой по ГОСТ 28147—89?

2.4. Библиографический список

2.4.1. Основная литература

2.4.1.1. Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223с.
2.4.1.2. Тепляков И.М. Основы построения телекоммуникационных систем и сетей: учебное пособие / И. М. Тепляков. - М. : Радио и связь, 2004. - 328 с.
2.4.1.3. Максименко В. Н. Защита информации в сетях сотовой подвижной связи. / В. Н. Максименко, В. В. Афанасьев, Н. В. Волков ; под ред. О. Б. Макаревича. - М. : Горячая линия - Телеком, 2007. - 360 с.

2.4.1.4. Романец Ю. В., П**. А.** Тимофеев, В. Ф. Шаньгин; Защита информации в компьютерных системах и сетях/ под ред. В. Ф. Шаньгина - 2-е изд., перераб. и доп. - М. Радио и связь 2001 - 376 с. ил.

2.4.1.5. Конспект лекций по курсу «Защита информации в системах беспроводной связи»

1.5.2. Дополнительная литература

1.5.2.1. С.В. Кунегин. Системы передачи информации. Курс лекций. - М. В/ч 33965, 1997, - 317 с.

1.5.2.2. Основы теории радиоэлектронной борьбы/под ред. Н.Ф. Николенко. - М. Военное издательство. 1987. – 351 с.

1.5.2.3. Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.

1.5.2.4. РД. АС. Защита от НСД к информации. Классификация АС и требования по защите информации. – М.: Гостехкомиссия России, 1992.