Практическая работа № 3

Защита информации в системах беспроводной связи путем имитозащиты передаваемых сообщений

3.1 Цель практической работы.

Цель практической работы состоит в ознакомлении с методом защиты информации в системах беспроводной связи путем имитозащиты передаваемых сообщений.

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

В результате выполнения практического задания студенты должны освоить метод защиты информации в системах беспроводной связи путем имитозащиты передаваемых сообщений.

3.2.Краткие теоретические сведения

Имитозащита передаваемых сообщений

В теории защиты информации рассматривается защита от двух классов воздействий - случайных и преднамеренных. Защита информации, передаваемой по каналам связи, от случайных помех осуществляется с помощью её ***помехоустойчивого кодирования***. При таком кодировании в информацию вносится избыточность (добавляется контрольная сумма, вычисленная по определённому алгоритму), и на приёмном конце с использованием этой избыточности производится обнаружение и/или исправление ошибок, внесённых в сообщение при его передаче.

Однако с помощью помехоустойчивого кодирования трудно обеспечить защиту от преднамеренных воздействий на сообщение, так как алгоритмы кодирования являются открытыми и известны злоумышленнику. В этом случае он может модифицировать сообщение и затем вновь вычислить контрольную сумму, а затем передать изменённое сообщение получателю. Он также может навязывать ложную информацию, создавая собственные сообщения, кодируя их помехоустойчивым кодом и передавая их в канал связи.

Защита канала шифрованной связи от навязывания ложной информации носит название ***имитозащиты.***

Для обеспечения имитозащиты необходимо, чтобы злоумышленник не имел возможности создавать правильные сообщения (то есть те, которые на приёмном конце канала будут восприняты как правильные).

Это возможно путём внесения избыточности в сообщения подобно тому, как это делается в случае защиты от случайных

помех. В этом случае алгоритм внесения избыточности должен быть скрыт от злоумышленника. Обычно процедура защиты строится на основе некоторой криптографической системы. К сообщению добавляется отрезок информации фиксированной длины, вычисленный по определённому правилу на основе открытых данных и ключа, называемый ***имитовставкой***. В открытые данные, используемые для выработки имитовставки, помимо собственно текста сообщения может быть включена и служебная информация, такая как дата и время отправки сообщения, регистрационный номер сообщения и так далее. В этом случае можно обеспечить также защиту от повторной передачи ранее переданного правильного сообщения.

Обеспечение имитозащиты по такой схеме предусмотрено ГОСТ 28147.

Имитозащита передаваемых сообщений осуществляется криптографическим способом. Для этого к передаваемому сообщению добавляются избыточные биты для обнаружения ошибок в приемном устройстве. Каждый избыточный бит должен зависеть от значений всех информационных бит. На информационные и избыточные биты накладывается шифрпоследовательность, в качестве которой может служить ***m***-последовательность.

В этом случае для создания ложного сообщения, подменяющее передаваемое сообщение злоумышленник должен передать некие ***к*** информационные биты и правильно угадать для этих ***к*** бит необходимые значения ***r*** избыточных бит. Вероятность этого события есть $P_л = (1/2)^r$.

Функциональная схема передачи сообщений с криптозащитой по линии связи приведена на рис. 3.1

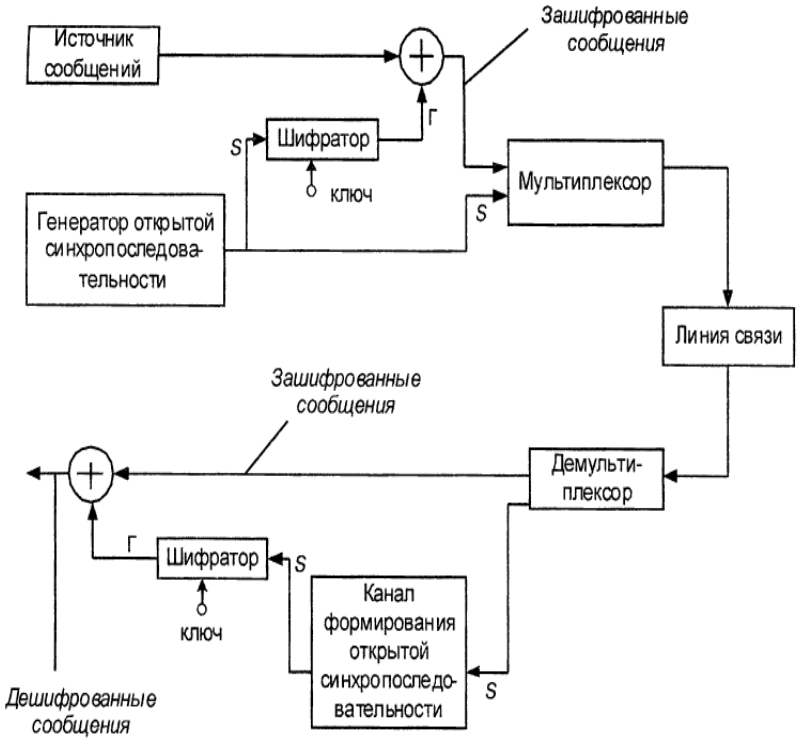

Рис. 3.1. Функциональная схема передачи сообщений с криптозащитой по линии связи:

S – двоичная синхропоследовательность, Г – двоичная последовательность с выхода шифратора

3.3. Практическое задание

1. При передаче команд управления полетом летательного аппарата требуется обеспечить имитозащиту передаваемых команд с вероятностью ложного формирования команды не более 10^{-9}:

а) При криптографическом способе обеспечения имитозащиты определить число избыточных бит кода с обнаружением ошибок, которое нужно передавать с каждой командой.

б) Какие дополнительные кодовые методы защиты передаваемых команд можно предложить для стирания наших команд, принятых злоумышленником и ретранслированных им через некоторое время для дезорганизации работы командной радиолинии?

3.4. Контрольные вопросы

1. Защита от каких классов воздействий рассматривается в теории защиты информации?
2. Как осуществляется защита информации, передаваемой по каналам связи, от случайных помех?
3. Как осуществляется защита информации, передаваемой по каналам связи, от преднамеренных помех?
4. Что такое имитозащита?
5. В чем состоит сущность имитозащиты?
6. Что такое имитовставка?
7. Чему равна вероятность правильного угадывания злоумышленником значений избыточных бит информации?

3.4 .Библиографический список

3.4.1. Основная литература

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. Тепляков И.М. Основы построения телекоммуникационных систем и сетей: учебное пособие / И. М. Тепляков. - М. : Радио и связь, 2004. - 328 с.
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.
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.
5. Конспект лекций по курсу «Защита информации в системах беспроводной связи»

3.4.2. Дополнительная литература

1. Теория электрической связи: учебное пособие / К.К. Васильев, В.А. Глушков, А.В. Дормидонтов, А.Г. Нестеренко;под общ. ред. К.К. Васильева. – Ульяновск: УлГТУ, 2008. – 452 с.

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

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

4. 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.
5. РД. АС. Защита от НСД к информации. Классификация АС и требования по защите информации. – М.: Гостехкомиссия России, 1992.