УДК 621.311

РАЗРАБОТКА МАКЕТА УСТРОЙСТВА ДИНАМИЧЕСКОЙ ГЕНЕРАЦИИ КЛЮЧЕЙ ШИФРОВАНИЯ ДЛЯ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ СВЯЗИ

А.В. Карпов, И.Р. Каюмов, А.Д. Смоляков

В работе представлена разработка приемопередающей аппаратуры для динамической генерации и распределения ключей симметричного шифрования. Принцип действия разрабатываемой аппаратуры основан на использовании случайности траектории распространения радиоволн в многолучевой среде. Разработанная аппаратура позволяет проводить когерентные измерения фазы несущей в гигагерцовом диапазоне, что дает возможность использовать эти измерения для технической реализации систем криптографической связи.

Ключевые слова: Приемный тракт, передающий тракт, фаза, фазовый детектор, опорный сигнал, синтезатор опорной частоты.

Введение

Генерация и распределение ключей шифрования/дешифрования между абонентами информационных систем является актуальной проблемой защиты информации. В связи с этим, существует потребность в устройствах, осуществляющих данные операции [1].

Целью данной работы является разработка и испытания аппаратуры для динамической генерации и распределения ключей симметричного шифрования, подлежащим непредсказуемым изменениям во времени. Принцип действия разрабатываемой аппаратуры основан на использовании случайности траектории распространения радиоволн в многолучевой среде [2]. Фаза принимаемого сигнала в такой среде будет также случайной величиной. Взаимность прямого и обратного распространения радиоволн позволяют считать одинаковыми значения фазы сигналов, регистрируемых на обоих концах радиоканала. В результате последо-вательности измерений случайной фазы многолучевого сигнала на двух концах радиолинии накапливают два совпадающих набора случайных чисел. Последнее позволяет сформировать два экземпляра ключа симметричного шифрования. Для реализации изложенного способа генерации и распределения ключей требуется создать устройство, осуществляющее двусторонний обмен служебными сигналами, а также когерентные измерения их фазы на несущей частоте. Достижение поставленной цели требует решение следующих двух основных задач:

- разработка приемопередающего оборудования для системы криптографической связи (передатчика, приемника, модуля автоматического измерения фазы, антенного коммутатора, блока синтеза опорных частот);
- реализация когерентных измерений фазы сигнала.

Описание устройства

На рисунке 1 представлена блок-схема разработанного приемопередающего (ПП) блока. Блок функционально разделяется на три части: передающий тракт, приемный тракт и автоматизированный измеритель фазы, каждый из которых задействуется в зависимости от работы блока ПП либо в режиме передатчика, либо в режиме приемника.

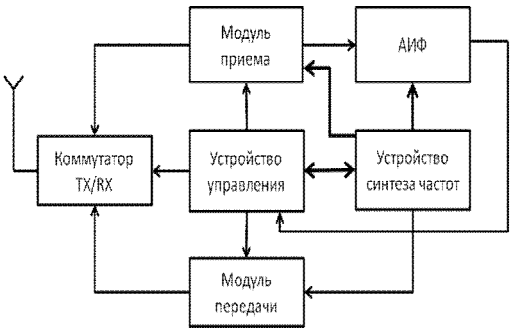

Рисунок 1 – Блок-схема приемопередающего блока

В состав передающего тракта входят: устройство синтеза частот, модуль передачи (МП), электронный антенный коммутатор, антенна. Приемный тракт содержит: антенну, электронный антенный коммутатор, модуль приема (МПР), устройство синтеза частот (УСЧ).

При установке блока в определенный режим работы устройство управления (УУ), реализованное на базе микроконтроллера,

загружает в оперативную память необходимую подпрограмму управления, в соответствии с которой производится конфигурация узлов блока. Антенный коммутатор (АК) производит мультиплексирование антенны по времени между приемным и передающим трактами. Устройство синтеза частот выполняет функции подсистемы синхронизации всех функциональных узлов блока. Антенный коммутатор АК реализован на базе специализированной микросхемы мультиплексора. Микросхема АК управляется потенциалом, формируемым УУ. При подаче на вход управления АК высокого уровня происходит подключение антенны к выходу передатчика, а при подаче низкого уровня потенциала – к входу приемника соответственно.

Рассмотрим порядок работы ПП в режиме передатчика[4]. Переход ПП в режим передатчика начинается с подключения антенны к передающему тракту при помощи коммутатора АК, управляемого сигналом УУ. Функции управляемого задающего генератора выполняет УСЧ. Сгенерированный УСЧ зондирующий сигнал усиливается до необходимого уровня МП и через электронный коммутатор АК поступает на передающую антенну, а далее излучается в многолучевый радиоканал.

Режим приема служебных сигналов реализуется по схеме приемника супергетеродинного типа[5]. При этом электронный коммутатор АК подключает антенну к приемному тракту. С выхода АК принятый сигнал подается на вход МПР, состоящий из двух каскадов УВЧ, смесителя и усилителя промежуточной частоты (УПЧ). Сигнал ПЧ с выхода МПР, несущий информацию о случайной фазе принятого служебного сигнала, подается на модуль автоматизированных измерений фазы (АИФ) и сравнивается с опорным сигналом от УСЧ. На выходе АИФ образуется постоянный уровень напряжения U, пропорциональный разности фаз φ сигналов на двух его плечах. Образующийся постоянный уровень напряжения U оцифровывается с помощью интегрированного АЦП и записывается в память микроконтроллера УУ. В память УУ также закладывается характеристика управления АИФ U(φ), позволяющая перевести записанный отсчет U в отсчет фазы принятого сигнала φ. Результирующий отсчет случайной фазы φ далее может быть записан в специальную область памяти для дальнейшего использования в целях генерации ключей симметричного шифрования.

Для реализации предусмотренных функций приемопередающего блока был разработан комплекс из семи подпрограмм управления, загружаемых в оперативную память УУ в зависимости от режима работы. Выбор режима может осуществляться при помощи управляющих клавиш блока. При включении устройства происходит начальная инициализация функциональных узлов, а также переход блока в режим генерации и передачи по многолучевому радиоканалу служебных сигналов на несущей частоте f0 = 952 МГц.

При работе ПП-блока в режиме передатчика происходит отключение ряда устройств (УВЧ, УПЧ, смесителя, DDS-синтезатора), входящих в состав приемного тракта. Это позволяет повысить мощность передачи полезного сигнала за счет снижения общего токопотребления, а также существенно уменьшить эффект паразитной модуляции несущей частоты со стороны синтезаторов частот, входящих в состав приемного тракта. Режим передатчика может быть прерван внешним сигналом, в качестве которого могут выступать либо нажатия на управляющие клавиши, либо прием служебного сигнала от аналогичного приемопередающего блока. При регистрации внешнего сигнала происходит формирование определенного аппаратного прерывания и вызов подпрограммы его обработки.

Разработанное устройство обеспечивает следующие характеристики:

Чувствительность приемника: 5 мкВ.

Диапазон принимаемых частот: 940 – 960 МГц

Выходная мощность передатчика: от 1 до 30 мВт.

Напряжение питания: от 6 В до 15 В по постоянному току.

Потребляемый ток: не более 300 мА.

Интерфейс управления/передачи данных: USB, UART.

Частота снятия фазовых измерений: до 100 кГц;

Точность измерения фазы: ±8° (при отношении (сигнал/шум) не менее 21 дБ и усреднении измерения фазы по 10 отсчетам);

Шаг перестройки рабочей частоты: 0,1 МГц.

Испытания устройства

Для проверки работоспособности макетов приемопередающего устройства были проведены их натурные испытания.

Целью испытаний являлось:

проверка работы блока АИФ;

экспериментальное подтверждение соблюдения фазовой взаимности;

Важным условием для корректной работы устройств является синхронизация опорных сигналов макетов. В проведенных экспериментах синхронизация приемопередающих устройств производилось с по-

мощью кабеля, которым соединялись оба макета.

Проверка работы блока АИФ происходила следующим образом: макеты приемопередатчиков были расположены на расстоянии 30 см друг от друга. Один из макетов работал в режиме передатчика, а другой в режиме приемника. На приемнике функционировал блок АИФ, который проводил измерение разности фаз принятого и опорных сигналов.

При нажатии кнопки на приемнике происходил сдвиг фазы опорного сигнала на 10 градусов и оцифровка уровня напряжения с модуля АИФ. Дальше оцифрованные значения напряжения передавались на компьютер через последовательный интерфейс UART.

Для обработки принимаемых компьютером данных была написана программа на языке C++. Эта программа обрабатывает данные, полученные из соответствующих последовательных портов (com-портов) и сохраняет их в во внутреннем буфере. В процессе поступления данных на компьютер, программа выводит их на экран.

Результаты градуировки блока АИФ представлен на рисунке 2. Некоторая асимметрия графика объясняется различием сравниваемых сигналов по амплитуде.

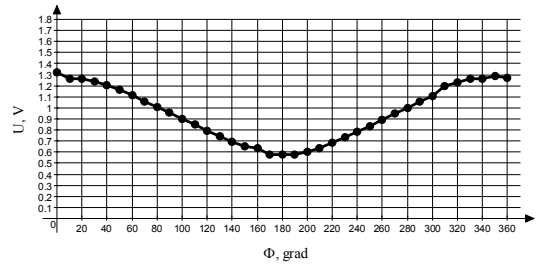

Рисунок 2 – градуировочный график блока АИФ

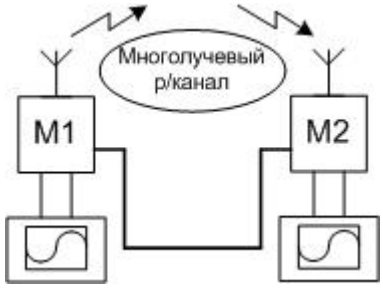

Рисунок 3 – Схема эксперимента

Для экспериментального подтверждения взаимности радиоканала были проведены сравнения параметров сигналов, принимаемых обоими макетами. Оценка различий параметров производилась путем визуальных наблюдений за амплитудно-фазовыми изменениями принятого сигнала по экрану осциллографа. При этом каждый макет был подключен к измерительному осциллографу. Схема эксперимента приведена на рисунке 3.

Макеты были размещены на расстояние 2,5м. друг от друга. После произведена двухсторонняя передача зондирующих сигналов и зафиксировано значение фазы между принятым и опорным сигналами.

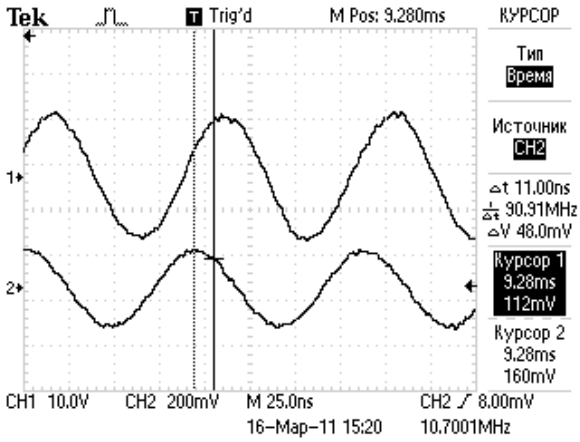

Рисунок 4 – Осциллограмма принятого и опорного сигнала для макета 1

Фаза принятого сигнала (относительно опорного) может быть определена осциллографическим методом. На рисунках 4 и 5 представлены примеры экспериментальных осциллограмм принятого (верхняя кривая) и опорного (нижняя кривая) сигналов. При этом фаза принятого сигнала составила 42° (рисунок 4) и 170° (рисунок 5).

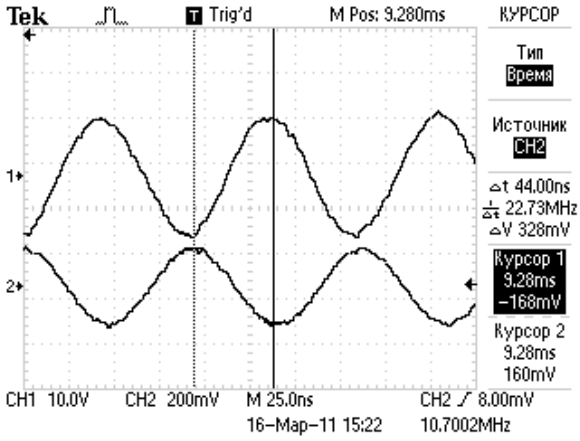

Рисунок 5 – Осциллограмма принятого и опорного сигнала для макета 2

Синхронизация обоих макетов приемопередатчиков от единого опорного генератора позволило исключить влияние нестабильности его частоты на точность измерений фазы. Поэтому основная ошибка результатов измерений определяется субъективной погрешностью оператора при снятии курсорных измерений по экрану осциллографа (порядка 5 нс). С учетом поправки на время распространения опорного сигнала по синхронизирующему кабелю (33 нс) данные, полученные от обоих макетов, совпадали в пределах указанной выше точности.

Выводы

В ходе проделанной работы были разработаны основные блоки устройства мобильной криптографической связи. Проведены натурные испытания приемопередающих блоков макетов данного устройства, в результате которых зарегистрировано соблюдение условий взаимности радиоканала в пределах обеспеченной аппаратурной точности измерений.

СПИСОК ЛИТЕРАТУРЫ

1. Сидоров В.В., Шерстюков О.Н., Сулимов А.И. Способ защиты информации. Заявка на изобретение № 2008152523, опубл. 10.07.2010 Бюл. № 19
2. Связь с подвижными объектами в диапазоне СВЧ / под ред. У.К. Джейкса. М.: Связь, 1979. 520 с.
3. Э. Ньюмен, С. Массе Проектирование приемника для систем WIMAX с дискретизацией промежуточной частоты, полученной после двойного преобразования с понижением частоты / Под ред. Н. Хамзина: Пер. с англ. // Беспроводные технологии. – 2008, № 03. – с. 58-64.
4. Козырев В.Б. Радиопередающие устройства. 3-е, доп. М.: Радио и связь, 2003. 560 с.
5. Бобров Н.В. Радиоприемные устройства. Изд. 2-е, доп. М.: Энергия, 1976. 368 с.

д.ф.м.н., проф. ***А.В. Карпов*** *– Arkadi.Karpov@ksu.ru; магистрант* ***И.Р. Каюмов*** *– ILNUR655@mail.ru; аспирант* ***А.Д. Смоляков*** *– alex9975@gmail.com; – Казанский федеральный университет, Институт Физики, кафедра радиофизики.*