УДК 621.311

РАЗРАБОТКА СРЕДСТВ БЕСПРОВОДНОЙ СИНХРОНИЗАЦИИ СИСТЕМЫ ДИНАМИЧЕСКОЙ ГЕНЕРАЦИИ КЛЮЧЕЙ ШИФРОВАНИЯ

А.В. Карпов, Р.Р. Фатыхов, А.Д. Смоляков

В статье описан способ беспроводной синхронизации системы динамической генерации ключей шифрования. Обоснован нижний предел нестабильности частоты опорных генераторов. В качестве опорных генераторов выбраны рубидиевые стандарты частоты, разработан и реализован протокол сетевой синхронизации

Ключевые слова: криптография, многолучевой радиоканал, распространение секретных ключей, синхронизация, частотная нестабильность, стандарт частоты

Актуальность

В настоящее время большинство криптографических методов основываются на математической теории сложности вычислений, которая не может гарантировать абсолютной защиты информации. По этой причине разработка физических методов шифрования, основанных на случайности протекания какого-либо физического процесса, является актуальной задачей.

Принцип шифрования основан на использовании случайности траектории распространения радиоволн в многолучевой среде [1]. На обоих концах радиолинии, во встречном режиме, одновременно проводятся измерения фазы монохроматического сигнала. Вследствие взаимности многолучевого радиоканала эти измерения с высокой точностью будут совпадать и на их основе можно сформировать два идентичных случайных ключа симметричного шифрования.

Для реализации изложенного способа шифрования была разработана аппаратура, осуществляющая когерентное измерение фазы сигналов во встречном режиме [2], в которой генерация ключей обеспечивается высокоточной синхронизацией. При проектировании системы синхронизации следует решить две основные задачи: как передавать синхросигнал от одного узла к другому и как организовать распределение синхросигналов по всем узлам системы [3]. Обе задачи синхронизации на данный момент осуществляются с помощью коаксиального кабеля, тем самым ограничивается возможность пространственного разнесения абонентов.

Целью данной работы является перевод системы динамической генерации и распределения ключей симметричного шифрования к беспроводному типу синхронизации. Для этого необходимо:

- рассмотреть варианты осуществления беспроводной синхронизации с учетом производительности системы;
- обеспечить устройства стабильными, синхронизированными опорными генераторами;
- разработать протокол синхронизации устройств.

Описание устройства

Блок-схема макета разработанного приемопередающего устройства представлена на рисунке 1. Схема функционально разделяется на две части: передающий тракт и приемный тракт, которые задействуются в соответствующем режиме работы (режим приема или передачи). В состав передающего тракта входят: блок синхронизации (БС), усилитель мощности (УМ), электронный антенный коммутатор (АК) и антенна. Приемный тракт включает в себя: антенну, электронный антенный коммутатор, усилитель высоких частот (УВЧ), фильтр высоких частот (ФВЧ), смеситель, фильтр промежуточной частоты (ФПЧ), усилитель промежуточной частоты (УПЧ), фазовый детектор (ФД), синтезатор частоты (DDS) и блок синхронизации. При установке устройства в определенный режим работы, устройство управления (УУ), реализованное на базе микроконтроллера ATmega169, загружает в оперативную память необходимую подпрограмму, в соответствии с которой производится конфигурация узлов устройства. Антенный коммутатор производит мультиплексирование антенны по времени между приемным и передающим трактами. В качестве блока синхронизации используется микросхема AD9548, на вход которой подается опорный сигнал 10 МГц от рубидиевого стандарта частоты (СЧ). Блок синхронизации обеспечивает стабильной частотой все узлы системы.

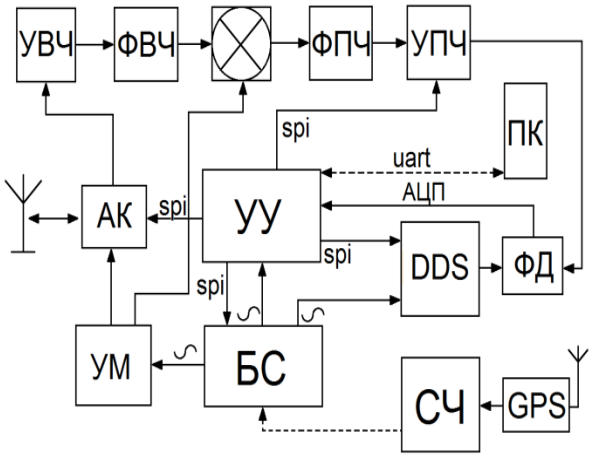

Рисунок 1 – Блок-схема приемопередающего устройства

Характеристики разработанного устройства следующие:

- Диапазон рабочих частот: 940 — 980 МГц;
- Шаг перестройки рабочей частоты: 0,1 МГц
- Чувствительность приемника: 5 мкВ;
- Выходная мощность передатчика: от 1 до 30 мВт;
- Напряжение питания: от 6 В до 15 В по постоянному току;
- Потребляемый ток: не более 500 мА;
- Интерфейс управления/передачи данных: USB, UART;
- Частота снятия фазовых измерений: до 100 кГц;
- Точность измерения фазы ±8º (при отношении сигнал/шум не менее 21 дБ и усреднении измерения фазы по 10 отсчетам);

Беспроводная синхронизация

При синхронизации по кабелю организация сеанса зондирования происходит в результате подачи стробирующего стартового импульса по кабелю от одного макета на устройство управления другого макета. Переходя к беспроводному типу синхронизации, необходимо обеспечить устройства тактовой синхронизацией, синхронизацией внутренних часов устройств и разработать протокол синхронизации.

Основной характеристикой радиоканала, влияющей на производительность криптосистемы, является нестабильность частоты опорных генераторов. На рисунке 2 представлен график зависимости количества бит ключевой последовательности (генерируемых из одного измерения фазы сигнала) от показателя нестабильности опорных генераторов для несущей частоты, равной 963МГц. Из графика видно, что для генерации хотя бы одного бита ключа из одного измерения фазы необходим источник опорного сигнала с показателем кратковременной нестабильности, равным 3×10^{-10} за 1 с. Это значение было принято за нижний предел качества опорного генератора.

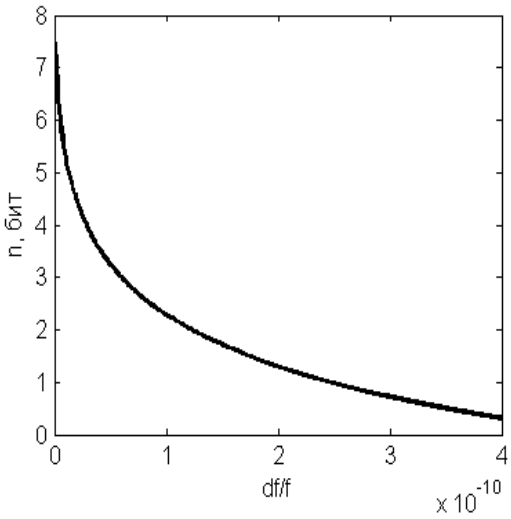

Рисунок 2 – График зависимости количества бит ключевой последовательности, генерируемых из одного измерения фазы сигнала, от показателя нестабильности опорного генератора

В качестве опорных генераторов было решено использовать рубидиевые стандарты частоты FS725. Стандарты частоты обладают показателем кратковременной нестабильности не более 2×10^{-11} за 1 с. За опорный сигнал берется синусоидальный сигнал 10 МГц (максимальная частота на выходе FS725). Для подстройки частот двух стандартов FS725 используется возможность корректировки параметров рубидиевой ячейки по интерфейсу RS-232. Диапазон подстройки частоты составляет ±0,02 Гц, с точностью до 1×10^{-5} Гц. Альтернативным вариантом подстройки частоты является возможность синхронизации сигналов с выхода FS725 сигналами приемников систем глобального позиционирования GPS/ГЛОНАСС. Что позволяет подстроить опорный сигнал к меткам времени 1 Гц с приемников GPS, которые обладают относительной долговременной нестабиль-

ностью вплоть до 10^{-12}. В результате подстройки частоты первым способом, фаза одного стандарта частоты относительно другого бежит со скоростью 1×10^{-3} Гр./с., что позволяет производить когерентные измерения в течение 15 минут, после чего необходимо подстроить регистрируемую фазу одного из макетов. В случае синхронизации частоты двух FS725 по сигналам спутников GPS в течение суток, пропадает необходимость подстройки регистрируемой фазы.

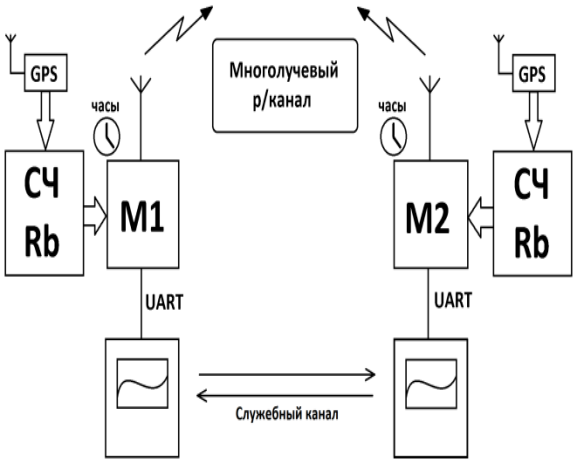

Рисунок 3 – Блок-схема беспроводной синхронизации двух макетов

На рисунке 3 представлена блок схема экспериментальной установки, состоящей из двух макетов с подключенными к ним стандартами частоты FS725, GPS приемниками и ПК с соответствующим программным обеспечением.

На базе микроконтроллера устройства управления (ATmega169) были реализованы внутренние часы, по которым осуществляется старт зондирования в заранее установленное время. В качестве опорного генератора часов используется дополнительный выход 1 Гц стандарта частоты FS725. При поступлении секундного импульса на вход часов происходит увеличение значения часов на единицу. Таким образом, достигается точность хода часов порядка 10 нс. На рисунке 4 представлена осциллограмма, показывающее расхождение во времени импульсов 1 Гц с двух стандартов частоты. За синхронизацию значений внутренних часов устройств отвечает разработанный протокол синхронизации.

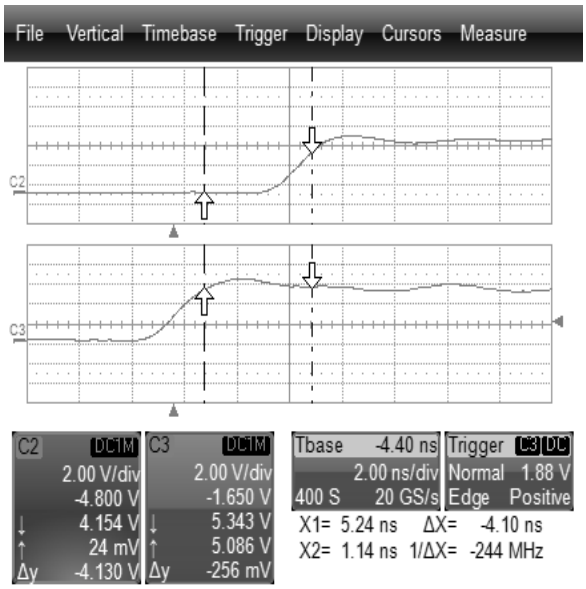

Рисунок 4 — Осциллограмма импульсов 1Гц с двух стандартов частоты

Протокол синхронизации организован в виде программы, написанной на языке Java. Программа, реализованная в рамках технологии клиент-сервер, устанавливает служебный канал связи, производит подстройку внутренних часов макетов и осуществляет корректировку текущих фаз фазометров. Интерфейс программы представлен на рисунке 5.

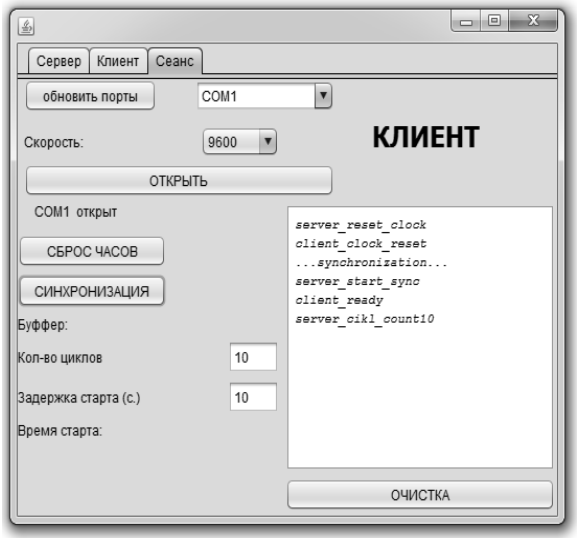

Рисунок 5 – Интерфейс программы синхронизации макетов

Связь макетов друг с другом происходит по Интернету с использованием протокола TCP/IP. На рисунке 6 представлена временная диаграмма протокола синхронизации.

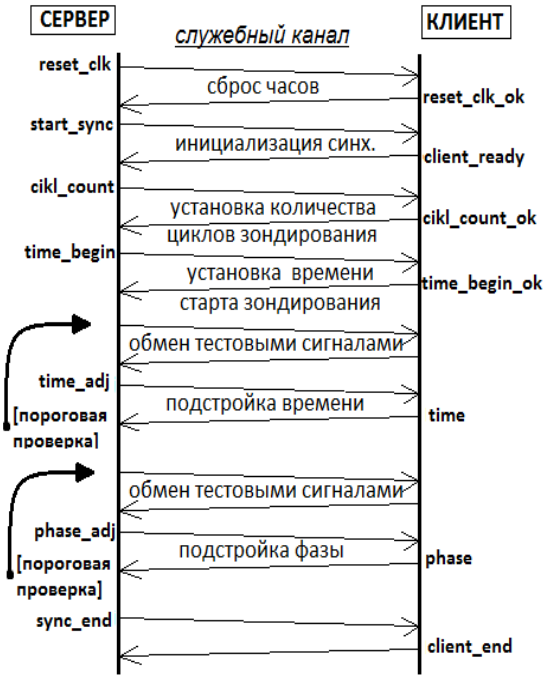

Рисунок 6 — Временная диаграмма протокола синхронизации

На первом этапе синхронизации происходит сброс внутренних часов устройств. Так как команда сброса от сервера клиенту доходит с определенной задержкой, часы клиента могут отставать от часов сервера на несколько секунд. Синхронизация часов происходит в результате обмена тестовыми сигналами и дальнейшей сверки с пороговым значением амплитуды. Регистрируемое значение амплитуды ниже порогового говорит о не совпадении (рисунок 7) интервалов приема/передачи (RX/TX). В случае если значение ниже порогового, к показаниям внутренних часов клиента добавляется 1 с. Процедура повторяется до тех пор, пока значение регистрируемой амплитуды не превысит пороговое, говоря о совпадении интервалов RX/TX и равенстве значений внутренних часов макетов. В результате вышеописанной процедуры, временные задержки передачи информации по служебному каналу не влияют на качество синхронизации, так как старт зондирования происходит по синхронизированным внутренним часам макетов в заранее установленное время.

Процедура подстройки начальных фаз фазометров происходит уже на синхронизированных макетах путем сравнения текущей выборки одного макета с выборкой другого. В результате подается корректирующее значение фазы на макет клиента. Подстройка фаз повторяется до тех пор, пока разность фаз не будет ниже заданного порогового значения.

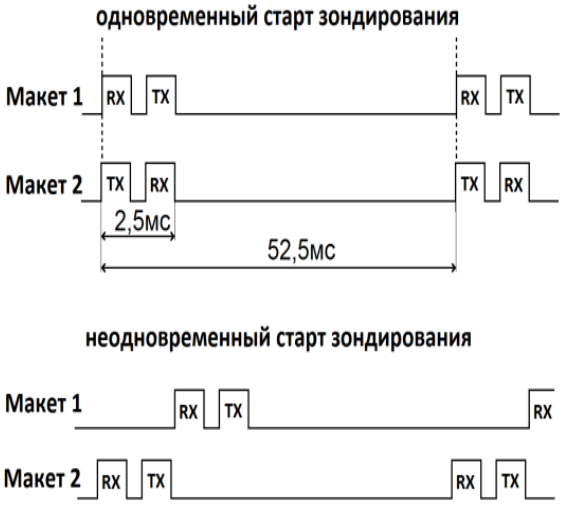

Рисунок 7 – Временная диаграмма обмена зондирующими сигналами

Выводы

Предложен и реализован способ беспроводной синхронизации пространственно разнесенных устройств генерации секретных ключей. В качестве опорных генераторов используются рубидиевые стандарты частоты FS725, имеющие возможность подстройки частоты к секундным меткам спутников GPS. Разработан протокол синхронизации позволяющий проводить когерентные измерения фазы с требуемой точностью.

СПИСОК ЛИТЕРАТУРЫ

1. Джейкс, У. Связь с подвижными объектами в диапазоне СВЧ [Текст] / У.К. Джейкс. – М.: Связь, 1979, – 384с.
2. Карпов, А.В. Разработка макета устройства динамической генерации ключей шифрования для криптографической системы связи [Текст] / А.В. Карпов, И.Р. Каюмов, А.Д. Смоляков // Ползуновский вестник. - 2011 - №. 3/1 - С. 210-213.
3. Брени, С., Синхронизация цифровых сетей связи [Текст] / С. Брени. под ред. проф. А.В. Рыжкова. -М.: Мир, 2003, -417с.

д.ф.-м.н., проф. ***А.В. Карпов*** — *Arkadi.Karpov@kpfu.ru; магистрант* ***Р.Р. Фатыхов*** — *ruslancomb@gmail.com; аспирант* ***А.Д. Смоляков*** — *alex9975@gmail.com: - Казанский федеральный университет, Институт Физики, кафедра радиофизики.*