

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

На правах рукописи



МИРОНОВ ЯКОВ КОНСТАНТИНОВИЧ

РАЗРАБОТКА АЛГОРИТМА СИНХРОНИЗАЦИИ СТАНЦИЙ
АВТОКОМПЕНСАЦИОННОЙ ВОЛОКОННО-ОПТИЧЕСКОЙ СИСТЕМЫ
КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА ОДНОФОТОННОМ
ЛАВИННОМ ФОТОДИОДЕ С РАЗБИЕНИЕМ ВРЕМЕННОГО КАДРА НА
ИНТЕРВАЛЫ

2.2.13. Радиотехника, в том числе системы и устройства телевидения

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель
доктор технических наук, профессор Румянцев К.Е.

Таганрог-2023

ОГЛАВЛЕНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	5
ВВЕДЕНИЕ	7
1. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ СИНХРОНИЗАЦИИ СТАНЦИЙ В СИСТЕМАХ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА	17
1.1 Особенности передачи информации в системах связи с применением квантовых технологий	17
1.2 Анализ специфики квантового распределения ключа	19
1.3 Исследование процесса синхронизации квантовых систем связи	26
1.4 Специфика однофотонной синхронизации станций квантового распределения ключа	32
1.5 Постановка общей научной задачи и формулировка частных задач диссертационных исследований	34
2. РАЗРАБОТКА ДВУХЭТАПНОГО АЛГОРИТМА СИНХРОНИЗАЦИИ С РАЗБИЕНИЕМ ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ НА УЧАСТКИ С УБЫВАЮЩЕЙ ДЛИНОЙ	37
2.1 Сравнительный анализ технических решений аппаратуры синхронизации	37
2.2 Синтез двухэтапного временного алгоритма синхронизации системы квантового распределения ключа	51
2.3 Обоснование типовой структуры программно-аппаратного комплекса для передачи конфиденциальной информации	56
2.4 Анализ структуры станций системы КРК с фазовым кодированием состояний фотонов по протоколу BB84	58
2.5 Техническое решение двухэтапного алгоритма однофотонной синхронизации	64
2.6 Выводы к главе 2	67

3. ОЦЕНКА ЭФФЕКТИВНОСТИ ДВУХЭТАПНОГО АЛГОРИТМА СИНХРОНИЗАЦИИ	69
3.1 Оценка вероятностных характеристик двухэтапного временного алгоритма синхронизации	69
3.2 Особенности разбиения волоконно-оптической линии на участки с убывающей длиной	73
3.3 Схемотехнические решения для опроса участков ВОЛС с убывающей длиной	84
3.4 Методика расчёта временных и энергетических характеристик двухэтапного временного алгоритма синхронизации	86
3.5 Методика расчёта условных вероятностных характеристик двухэтапного временного алгоритма синхронизации	93
3.6 Анализ временных характеристик на этапе тестирования в сигнальном участке ВОЛС	94
3.7 Методика расчёта времени тестирования при ложном решении на этапе поиска	98
3.8 Моделирование этапа тестирования при нахождении однофотонного источника излучения в сигнальном участке ВОЛС	100
3.9 Моделирование двухэтапного алгоритма синхронизации станций с разбиением волоконно-оптической линии на участки с убывающей длиной	105
3.10 Выводы к главе 3	109
4. СТАТИСТИЧЕСКАЯ ОЦЕНКА ВРЕМЕНИ ДВУХЭТАПНОЙ СИНХРОНИЗАЦИИ ПРИЁМОПЕРЕДАЮЩЕЙ И КОДИРУЮЩЕЙ СТАНЦИЙ СИСТЕМЫ КРК	112
4.1 Постановка задачи статистической оценки времени двухэтапной синхронизации приёмопередающей и кодирующей станций СКРК	112
4.2 Диаграмма состояний и переходов для случайного поиска	113
4.3 Определение статистических характеристик двухэтапного алгоритма графоаналитическим методом	115

4.4 Определение статистических характеристик этапа тестирования в шумовом участке ВОЛС	132
4.5 Определение статистических характеристик этапа тестирования в сигнальном участке ВОЛС	136
4.6 Выводы к главе 4	144
ЗАКЛЮЧЕНИЕ	146
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	148
ПРИЛОЖЕНИЕ А. ЛИСТИНГ ПРОГРАММ МАТЛАВ ДЛЯ ПРОЕКТИРОВАНИЯ МОДУЛЯ ДВУХЭТАПНОЙ ОДНОФОТОННОЙ СИНХРОНИЗАЦИИ	162
ПРИЛОЖЕНИЕ Б. СЕРТИФИКАТЫ	166
ПРИЛОЖЕНИЕ В. АКТЫ ВНЕДРЕНИЯ	170

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Квантовая криптография – методы защиты информации, использующие законы квантовой физики.

Распределение ключа – технология создания у двух удалённых пользователей строки случайных бит криптографического ключа.

Квантовое распределение ключа – технология распределения ключа на основе законов квантовой физики.

Сигнал в системах квантового распределения ключа – передаваемое состояние фотона.

Фотонный импульс – оптический импульс со средним числом фотонов менее одного.

Однофотонный импульс – отклик однофотонного фотодетектора на приём фотона.

Временное окно – временной интервал, в котором регистрируют фотоны.

Сигнальное временное окно – временной интервал, в котором располагается фотонный импульс.

Временной кадр – временной интервал, равный периоду следования оптических импульсов.

Синхронизация станций при квантовом распределении ключа – процесс согласования моментов генерации и регистрации фотонного импульса.

QKD	–	quantum key distribution
ВОЛЗ	–	волоконно-оптическая линия задержки
ВОЛС	–	волоконно-оптическая линия связи
ВОПС	–	волоконно-оптический поляризационный сплиттер
ВОФМ	–	волоконно-оптический фазовый модулятор
ГТИ	–	генератор тактовых импульсов
ЗФ	–	зеркало Фарадея
ИТТ	–	импульс темнового тока
КРК	–	квантовое распределение ключа

ЛЗ	—	линия задержки
НСД	—	несанкционированный доступ
ОЛФД	—	однофотонный лавинный фотодиод
ПОМ	—	передающий оптический модуль
ПРОМ	—	приёмный оптический модуль
УУ	—	устройство управления
ФИ	—	формирователь импульсов
ЦСИ	—	цифровой счётчик импульсов

ВВЕДЕНИЕ

Обеспечение секретности и конфиденциальности информации при передаче в системе связи является актуальной задачей. Для повышения безопасности передаваемых данных активно используется шифрование. Однако наряду с развитием технологий обеспечения безопасности информации развиваются технологии несанкционированного доступа (НСД). Одним из способов решения данной проблемы является использование квантовых технологий, в том числе систем квантового распределения ключа (КРК) [1].

Применение протоколов квантовой криптографии потенциально обеспечивает абсолютную секретность при шифровании сообщений и распределении секретного ключа между легитимными пользователями [1, 2, 3]. Однако техническое несовершенство оптоэлектронных компонентов синхронизации системы КРК потенциально упрощает злоумышленнику организацию НСД к информации или внесения помех [4, 5, 6, 7]. Для этого злоумышленник должен иметь информацию о точном времени стробирования (опроса) фотодетекторов приёмного блока станции [8, 9].

В [10] подчёркивается, что проблема временной синхронизации станций в оптических системах связи отличается от традиционной проблемы в системах радиосвязи с аддитивными гауссовскими шумами [11, 12, 13].

Подход к оценке эффективности синхронизации с учётом квантовой природы выходного сигнала фотодетектора развивается в [10]. С этих позиций проанализирован ряд алгоритмов и описаны типовые подсистемы синхронизации оптических систем связи. Показано, что для оптических систем связи наиболее подходящей формой синхросигнала является периодическая последовательность оптических импульсов. Причём синхронизация (оценка времени приёма синхроимпульса) включает по времени две операции. Первая операция грубой синхронизации сводится к дискретизации временного кадра, равного периоду следования синхроимпульсов, на интервалы (временные окна) и обнаружению

факта присутствия в одном из них синхросигнала. В процессе второй операции точной синхронизации осуществляются дополнительные временные сдвиги временного окна для определения точного местоположения синхросигнала на временной оси.

Однако анализ в [10] не ориентирован на оценку защищённости подсистемы синхронизации от НСД. Косвенно в пользу слабой защищённости приводимых здесь алгоритмов обнаружения может говорить тот факт, что для синхронизации используются многофотонные синхроимпульсы. Так, например, даже для обеспечения вероятности обнаружения синхроимпульса 0,9 при требовании вероятности ложных тревог 0,001 потребуется во временном кадре регистрировать в среднем 7 фотонов.

Реализация процесса синхронизации в многофотонном режиме потенциально упрощает злоумышленнику доступ к конфиденциальной информации. Кроме того, в этих условиях злоумышленник может вносить помехи в процесс КРК.

Для повышения защищённости подсистемы синхронизации от НСД предложен и обоснован принцип синхронизации приёмопередающей и кодирующей станций в автокомпенсационной системе КРК с использованием в качестве синхросигналов фотонных импульсов [14, 15] (однофотонный режим синхронизации), причём уровень сигнала составляет примерно 0,1 фотона на импульс (т.е. в среднем 1 фотон на 10 импульсов). Однако при однофотонном режиме передачи синхроимпульсов значительно сокращается протяжённость ВОЛС.

В связи с этим, разработка алгоритма синхронизации приёмопередающей и кодирующей станций системы КРК, обеспечивающего протяжённую ВОЛС при однофотонном режиме передачи синхроимпульсов, является актуальной задачей исследования.

Цель диссертационных исследований: увеличение протяжённости ВОЛС в автокомпенсационной системе КРК на ОЛФД при сохранении энергетической скрытности синхронизации на основе протокола BB84.

Объект исследований: автокомпенсационная система КРК по оптическому волокну на основе протокола BB84.

Предмет исследований: алгоритм двухэтапной синхронизации автокомпенсационной системы КРК в однофотонном режиме.

Общая научная задача: разработка и исследование алгоритма вхождения в синхронизм автокомпенсационной системы КРК на ОЛФД, гарантирующего протяжённую ВОЛС при сохранении энергетической скрытности синхронизации и обеспечении вероятности ошибки синхронизации не выше требуемого значения. Создание методик расчёта и основ проектирования подсистем синхронизации, защищённых от НСД.

Частные задачи диссертационных исследований:

- анализ подсистем синхронизации станций автокомпенсационных систем КРК в существующих коммерческих решениях. Обоснование актуальности, определение общей научной задачи и частных задач диссертационных исследований;

- синтез алгоритма синхронизации станций автокомпенсационной системы КРК с повышенной защитой от НСД, обусловленной применением однофотонного уровня передачи и двухэтапным определением момента появления фотонного импульса;

- определение аналитических выражений для расчёта энергетических, вероятностных и временных параметров алгоритма синхронизации станций автокомпенсационной системы КРК;

- моделирование процесса синхронизации автокомпенсационной системы КРК для доказательства эффективности разрабатываемого алгоритма.

Для решения поставленных задач используются следующие методы исследования:

методы теории обнаружения для синтеза алгоритма синхронизации системы КРК;

методы теории вероятностей, теории графов и математической статистики при выводе аналитических выражений для расчёта вероятностных характеристик системы КРК в режиме синхронизации;

численные методы для оценки влияния параметров аппаратуры поиска на вероятностные и временные характеристики на этапе синхронизации системы КРК;

компьютерное моделирование для доказательства эффективности и подтверждения реализуемости предлагаемого алгоритма синхронизации в автокомпенсационных системах КРК.

Основные научные положения, выдвигаемые для защиты:

Положение 1. Актуальной проблемой является поиск алгоритма синхронизации станций на однофотонных лавинных фотодиодах, гарантирующего протяжённость волоконно-оптической линии более 20 км при сохранении энергетической скрытности синхронизации и обеспечении вероятности ошибки синхронизации не выше требуемого значения.

Положение 2. Разработанные двухэтапный временной алгоритм и структура подсистемы синхронизации системы КРК обеспечивают значительное снижение влияния импульсов темнового тока (ИТТ) ОЛФД за счёт разбиения ВОЛС на участки с убывающей длиной.

Положение 3. Предложенный двухэтапный временной алгоритм синхронизации приёмопередающей и кодирующей станций системы КРК, отличительной особенностью которого является разбиение ВОЛС на участки с убывающей длиной, обеспечивает увеличение протяжённости ВОЛС при вероятности ошибки синхронизации не выше требуемого значения.

Положение 4. Полученные аналитические выражения обеспечивают возможность расчёта среднего времени синхронизации графоаналитическим методом при произвольном количестве участков, кадров и тестов согласно предложенному алгоритму синхронизации станций автокомпенсационной системы КРК при разбиении ВОЛС на участки с убывающей длиной.

К наиболее существенным новым научным результатам, полученным в результате диссертационных исследований, относятся:

– двухэтапный алгоритм синхронизации автокомпенсационной системы КРК, позволяющий увеличить протяжённость ВОЛС благодаря разбиению ВОЛС на участки с убывающей длиной при сохранении энергетической скрытности синхронизации;

– методика разбиения ВОЛС на участки с убывающей длиной при обеспечении вероятности ошибки синхронизации на верхней границе любого участка не выше допустимого значения;

– аналитические выражения для расчёта временных и вероятностных параметров при анализе любого участка ВОЛС на этапах поиска и тестирования в режиме синхронизации, в том числе аналитические выражения для расчёта среднего времени вхождения в синхронизм графоаналитическим методом при произвольном количестве участков, кадров и тестов;

– структура подсистемы предварительной однофотонной синхронизации для автокомпенсационной системы КРК согласно разработанному алгоритму синхронизации.

Научная новизна работы состоит в следующем:

Разработан новый двухэтапный алгоритм временной синхронизации приёмопередающей и кодирующей станций системы КРК, позволяющий увеличить протяжённость ВОЛС благодаря разбиению ВОЛС на участки с убывающей длиной при сохранении энергетической скрытности синхронизации и обеспечивающий вероятность ошибки синхронизации не выше требуемого значения (пункт 5 паспорта специальности).

Впервые получены аналитические выражения для расчёта вероятностных, временных и энергетических характеристик синхронизации согласно предложенному алгоритму при произвольном количестве участков, кадров и тестов (пункт 5 паспорта специальности).

Предложена структура подсистемы синхронизации, реализующая разработанный алгоритм синхронизации, обеспечивающий повышенную безопасность и гарантию увеличения протяжённости ВОЛС (пункт 16 паспорта специальности).

Практическая ценность работы заключается в следующем:

Предложен двухэтапный алгоритм синхронизации приёмопередающей и кодирующей станций системы КРК, позволяющий благодаря разбиению ВОЛС на участки с убывающей длиной увеличить протяжённость ВОЛС в разы при сохранении энергетической скрытности, по сравнению с известными однофотонными алгоритмами. Так, например, при вероятности ошибки синхронизации 0,01 протяжённость ВОЛС увеличивается почти в 6 раз (пункт 5 паспорта специальности).

Разработана методика разбиения волоконно-оптической линии на участки с убывающей длиной, где длина каждого последующего участка меньше длины предыдущего, причём вероятность ошибки синхронизации на верхней границе любого участка не превышает допустимого значения (пункт 16 паспорта специальности).

Разработаны методики расчёта вероятностных, временных и энергетических характеристик двухэтапного временного алгоритма синхронизации, в том числе методика расчёта среднего времени синхронизации системы КРК графоаналитическим методом при произвольном количестве участков, кадров и тестов (пункт 16 паспорта специальности).

Разработаны два программных продукта для ЭВМ, защищённые авторскими свидетельствами, позволяющие анализировать характеристики предложенного двухэтапного алгоритма синхронизации: оценивать характеристики каждого из участков ВОЛС с убывающей длиной, вероятностные и энергетические характеристики алгоритма, моделировать этап тестирования с оценкой временных и вероятностных характеристик (пункт 16 паспорта специальности).

Внедрение результатов работы.

Результаты диссертационных исследований, посвящённые увеличению протяжённости ВОЛС автокомпенсационной системы КРК на ОЛФД при сохранении энергетической скрытности синхронизации на основе протокола BB84, использованы при выполнении гранта РФФИ 20-37-90040 Аспиранты, «Разработка алгоритма синхронизации станций автокомпенсационной волоконно-оптической

системы квантового распределения ключа на однофотонном лавинном фотодиоде с разбиением временного кадра на интервалы».

Апробация работы.

Основные положения диссертационной работы докладывались и обсуждались на 4-х международных и 7 всероссийских научно-технических конференциях:

– the 3rd International Conference on System Reliability and Safety Engineering» (SRSE 2021), November 26-28, 2021, Harbin, China;

– 13th International Conference on Security of Information and Networks (SIN 2020), 4-7 November 2020, Istanbul, Turkey;

– International Conference on Futuristic Trends in Networks and Computing Technologies, FTNCT 2019, 22-23 November 2019, Chandigarh, India;

– International Conference on Futuristic Trends in Networks and Computing Technologies, FTNCT 2018, 9-10 February 2018, Solan, India;

– II Всероссийская научная конференция «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (FISP-2020), 30 Ноября 2020, Россия, г. Ставрополь;

– I Всероссийская научно-практическая конференция «Digital Era», 26 марта 2021 г., г. Грозный;

– Всероссийская научно-техническая конференция с международным участием имени профессора Пьявченко О.Н. “Компьютерные и информационные технологии в науке, инженерии и управлении” «КомТех-2020», 3-5 июня 2020 года, ЮФУ ИРТСУ, Ростовская обл. г.Таганрог;

– V-VIII Всероссийские научно-технические конференции молодых ученых, аспирантов, магистрантов и студентов «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности», 1-7.04.2019, 6-12.04.2020, 5-11.04.2021, 4-9.04.2022, Таганрог.

Публикации.

По результатам диссертационных исследований опубликовано 15 научных работ. Из них в перечне рецензируемых научных изданий, рекомендованных ВАК

Минобрнауки России для публикации материалов диссертаций на соискание ученых степеней кандидата и доктора технических наук, в соавторстве с научным руководителем Румянцевым К.Е., опубликованы 2 статьи [16, 17]. В реферируемых изданиях, учитываемых в РИНЦ, опубликовано 4 работы [18, 19, 20, 21]. В трудах международных конференций, реферируемых в базе данных «SCOPUS», апробированы 5 научных статей [22, 23, 24, 25, 26]. Получено 2 авторских свидетельства на программные продукты для ЭВМ [27, 28].

Структура диссертационной работы. Диссертационное исследование написано на русском языке, включает введение, четыре главы, заключение, список использованных источников и приложения. Полный объём диссертации составляет 169 страниц, включая 33 рисунка и 20 таблиц. Список литературы содержит 113 наименований. Приложения содержат 9 страниц.

Во введении рассмотрена актуальность исследования и разработки алгоритма синхронизации станций автокомпенсационной волоконно-оптической системы КРК на однофотонном лавинном фотодиоде, поставлена цель диссертационных исследований. Определены объект, предмет, общая научная задача и частные задачи диссертационных исследований. Установлены методы исследования, необходимые для решения поставленных задач. Отмечены наиболее существенные новые научные результаты, научная новизна, практическая ценность работы, а также внедрение её результатов. Указаны апробации результатов исследований и публикации.

В первой главе проведён анализ протоколов квантовой криптографии и обоснован выбор протокола BB84, определена структура автокомпенсационной системы КРК. Установлена связь качества функционирования систем КРК с подсистемой синхронизации приёмопередающей и кодирующей станций КРК. Обоснован однофотонный режим синхронизации станций, обеспечивающий безопасность процесса синхронизации от НСД. Отмечена актуальность разработки однофотонного алгоритма синхронизации станций системы КРК с увеличением протяжённости ВОЛС.

Во второй главе проанализированы технические решения, защищённые патентами, и структуры подсистем синхронизации. Обоснована целесообразность разработки алгоритма подсистемы синхронизации станций системы КРК с повышенной защищённостью с увеличением протяжённости ВОЛС. Синтезирован алгоритм синхронизации приёмопередающей и кодирующей станций с фазовым кодированием состояний фотонов в автокомпенсационной системе КРК. Отличительной особенностью алгоритма является разбиение ВОЛС на участки с убывающей длиной, что позволяет значительно уменьшить влияние импульсов темнового тока ОЛФД. Обоснована структура программно-аппаратного комплекса для передачи конфиденциальной информации посредством КРК. Проанализирована структура станции системы КРК MagiQ QPN 5505. Предложена структура подсистемы синхронизации станций в системе КРК согласно разработанному двухэтапному алгоритму, учитывающему параметры используемого ОЛФД.

В третьей главе получены аналитические выражения и разработана методика расчёта вероятностных, временных и энергетических характеристик предлагаемого двухэтапного алгоритма синхронизации. Разработана методика разбиения ВОЛС на участки с убывающей длиной при обеспечении вероятности ошибки синхронизации на верхней границе любого участка на заданном уровне. Моделированием двухэтапного алгоритма синхронизации приёмопередающей и кодирующей станций системы КРК доказана эффективность предлагаемого двухэтапного алгоритма синхронизации. При ухудшении требований к вероятности ошибки синхронизации, и, следовательно, увеличении протяжённости ВОЛС, отмечено значительное увеличение времени вхождения в синхронизм. Ужесточение требований к вероятности ошибки синхронизации позволяет достичь синхронизации станций системы КРК в 1-м участке ВОЛС с вероятностью более 99%.

В четвёртой главе предложен графоаналитический метод расчёта среднего времени вхождения в синхронизм станций системы КРК для предлагаемого двухэтапного алгоритма синхронизации приёмопередающей и кодирующей

станций системы КРК. Получены аналитические выражения для расчёта среднего времени синхронизации станций. Отклонение результатов расчёта среднего времени синхронизации, полученных с помощью графоаналитического метода, от результатов моделирования не превышает 2,8 %. Незначительное отклонение указывает на возможность использовать полученные аналитические выражения для расчёта среднего времени синхронизации станций системы КРК согласно предложенному алгоритму. Получены аналитические выражения для экспресс-расчёта среднего и дисперсии времени этапа тестирования, причём отклонение результатов при экспресс-расчёте от полученных ранее результатов составляет не более 5,89 % для среднего времени тестирования и не более 5,05 % для СКО, что указывает на возможность применения аналитических выражений для экспресс-расчёта среднего и дисперсии этапа тестирования. Отметим, отклонение расчётов при экспресс-методе относительно результатов моделирования составляет не более 3,1 %.

В заключении подведены итоги диссертационных исследований, обосновано достижение поставленной цели.

В приложениях приведены свидетельства о регистрации программных продуктов для ЭВМ, сертификаты участия в научных конференциях и акты внедрения результатов диссертационной работы.

1. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ СИНХРОНИЗАЦИИ СТАНЦИЙ В СИСТЕМАХ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА

1.1 Особенности передачи информации в системах связи с применением квантовых технологий

Обеспечение безопасности информации при передаче между легитимными пользователями в системах связи является одной из главных задач в быстро прогрессирующем мире. Стремительная информатизация привела к применению технологий, гарантирующих защищённость данных и скрытность от НСД.

Секретность конфиденциальной информации при передаче её по защищённым линиям связи обеспечивается использованием симметричных криптосистем, в которых важным критерием эффективности является безопасное распределение секретного ключа между пользователями [29]. Однако способы НСД к существующим классическим системам передачи информации стремительно совершенствуются. Классические протоколы криптографии основаны на вычислительной сложности, что не составляет значительной проблемы наряду с мощностью современных вычислительных машин.

Один из вариантов достижения абсолютной секретности при распределении ключа и шифровании передаваемых данных – использование квантовой криптографии [1, 30, 31, 32, 33, 34].

Анализируя тенденции развития систем КРК, необходимо отметить возможность кодирования в фотонах состояния фазы, поляризации или времени. Базовый принцип квантовой криптографии – принцип неопределенности Гейзенберга, который заключается в невозможности одновременного измерения с абсолютной точностью двух параметров частицы.

Это исключает копирование или скрытый перехват данных. Легитимные пользователи способны отличить наличие злоумышленника в линии связи, так как в случае НСД к информации, квантовое состояние фотонов изменится. При проверке наличия злоумышленника в линии связи легитимные пользователи

оценивают наличие ошибок в сообщении по сравнению с выбранным объёмом переданной информации.

С момента появления первого протокола КРК [2] предложены и продемонстрированы разные протоколы, которые можно разделить на два класса – протоколы с дискретной переменной (DV-QKD) и протоколы с непрерывной переменной (CV-QKD) [35, 36]. Протоколы DV-QKD, такие как BB84, B92 или когерентный односторонний (COW) [37], предполагают генерацию и обнаружение очень слабых оптических сигналов, в идеале на уровне одиночных фотонов. Ряд успешных технологий реализован через протокол DV-QKD, но обычно они сильно отличаются от технологий, используемых в классических коммуникациях [38]. С другой стороны, протоколы CV-QKD представляют интерес, поскольку они могут использовать традиционные телекоммуникационные технологии. Такой подход имеет потенциальные преимущества из-за способности достигать высокой скорости генерации секретного ключа при скромных технологических ресурсах. Особенностью протоколов CV-QKD является использование классического когерентного приёмника, который можно использовать для счёта фотонов. Существенным недостатком систем с CV-QKD является ограничение дальности передачи до 60 км, что меньше дальности передачи систем с DV-QKD [39]. Также скорость генерации секретного ключа CV-QKD ограничена полосой пропускания гомодинного детектора и эффективностью согласования, которая ухудшается из-за избыточного шума, наблюдаемого при высоких скоростях передачи данных [40]. Зависимости от расстояния скорости генерации секретного ключа для CV-QKD и DV-QKD систем показаны на рисунке 1.1 [41, 42]. Видно, что дальность передачи ключа в системах CV-QKD намного ниже, чем в системах DV-QKD. Таким образом, для обеспечения секретности и протяжённой линии связи при фотонной передаче данных целесообразно использовать системы с протоколами DV-QKD.

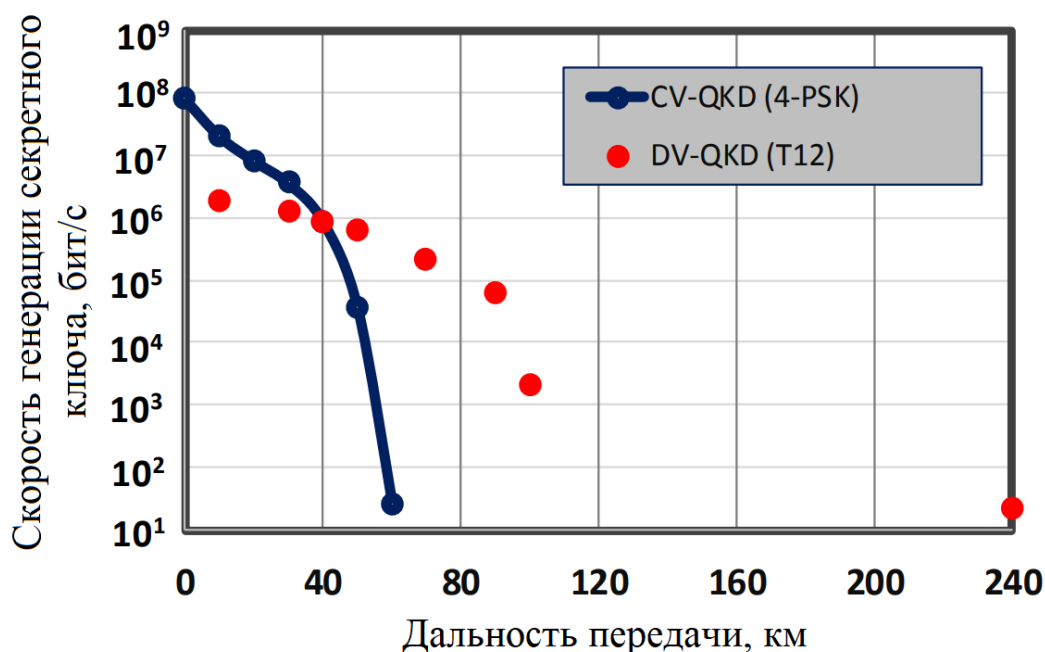


Рисунок 1.1 – Зависимости скорости генерации ключа от дальности передачи

Резюме. Теоретически абсолютная секретность передачи информации может быть реализована с помощью протоколов квантовой криптографии. Проанализированы протоколы DV-QKD с дискретной переменной и CV-QKD с непрерывной переменной. За основу для дальнейшего исследования взят класс протоколов с дискретной переменной DV-QKD, обеспечивающих генерацию секретного ключа на протяжённые расстояния.

1.2 Анализ специфики квантового распределения ключа

В системе КРК процесс формирования бит секретного ключа подчиняется конкретному протоколу [32]. Протоколы DV-QKD подразделяются на два подкласса: протоколы с кодированием состояний одиночных фотонов и с кодированием пары фотонов.

В основе протоколов с кодированием состояний одиночных фотонов лежит теорема о запрете клонирования неизвестного квантового состояния. Следовательно, попытки НСД к системе приводят к возникновению ошибок, которые будут обнаружены легитимными пользователями. Наиболее известные протоколы с кодированием состояний одиночных фотонов – BB84 [2], B92 [43], BB84 (4+2) [44], с шестью состояниями [45], Гольденберга–Вайдмана [46], Коаши–Имото [47], SARG04 [48].

Из-за сложности реализации, единственным протоколом на основе квантовой сцепленности пары фотонов является протокол E91. Отличительной особенностью протокола является источник пары запутанных частиц, которые посылаются Алисе и Бобу.

Наиболее распространёнными являются протоколы BB84 и B92. Протокол B92 использует передачу двух неортогональных состояний квантовой системы, в то время как в протоколе BB84 используются четыре квантовых состояния. При использовании протокола B92 значительно упрощается схема реализации, с другой стороны, снижается эффективность за счёт уменьшения количества принимаемых фотонов. Следовательно, протяжённость передачи секретного ключа сокращается и составляет около 20 км, что значительно уступает протоколу BB84 [30].

Таким образом, для достижения достаточно протяжённой линии передачи секретных ключей оптимально применение протокола BB84.

В зависимости от модуляции состояний одиночных фотонов различают протоколы BB84 с поляризационной, фазовой и временной модуляцией состояний фотонов. Реализация протокола BB84 с поляризационной модуляцией состояний фотонов не нашла широкого применения из-за технических сложностей компенсации изменений поляризации излучения при распространении через волоконно-оптическую линию связи (ВОЛС). При временной модуляции состояний фотонов для согласования базиса требуется пересылка двух бит классической информации вместо одного. Широкое распространение протокол BB84 получил с фазовой модуляцией состояний фотонов, обеспечивая рекордные протяжённости ВОЛС. Присутствие сложной технической проблемы из-за требований стабилизации и синхронизации [30] обуславливает выбор для анализа системы КРК с фазовым кодированием состояний фотона.

Известен ряд систем КРК [49, 50, 51, 52, 53, 54, 55]. Активно ведутся исследования для улучшения характеристик систем передачи, увеличения протяжённости линии связи и скорости формирования квантового ключа.

Разработаны системы КРК компаниями MagiQ (США), ID Quantique (Швейцария), AIT (Австралия), SeQureNet (Франция), IBM, Smart Quantum (США),

GAP-Optique (Швейцария), Toshiba (Япония), Mitsubishi (Япония), а также холдингом QinetiQ, национальной лабораторией в Лос-Аламосе и Калифорнийским технологическим институтом [43, 44, 46, 47, 56, 57].

Системы id 500 Clavis и id 3000 Clavis компании ID Quantique состоят из приёмопередающей (Боб) и кодирующей (Алиса) станций. Процесс КРК проводится в автоматическом режиме. Система id 3000 Clavis поддерживает два протокола (BB84 и SARG04), генерируя секретные ключи через квантовый канал протяжённостью до 100 км со скоростью до 1500 бит/с [58]. На рисунке 1.2 представлена структурная схема приёмопередающей станции системы id 3000 Clavis [59]. Станция включает передающий оптический модуль (ПОМ), волоконно-оптический циркулятор, два приёмных оптических модуля (ПрОМ_{Б1} и ПрОМ_{Б2}), оптический делитель X-типа с коэффициентом деления 50/50, первую волоконно-оптическую линию задержки (ВОЛЗ_Б), 1-й волоконно-оптический фазовый модулятор (ВОФМ_Б) и волоконно-оптический поляризационный ответвитель (ВОПО). Функциональные элементы соединены между собой оптоволоконном с сохранением поляризации. Необходимо отметить, система работает в многофотонном режиме.

На рисунке 1.3 представлена структурная схема кодирующей станции системы id 3000 Clavis [59]. Станция включает ответвитель Y-типа с коэффициентом деления 1:9 между портами 2 и 3, два регулируемых волоконно-оптических аттенюатора (ВОА_{А1} и ВОА_{А2}), ВОЛЗ_А, ВОФМ_А, зеркало Фарадея и оптоволоконно (ОВ), соединяющее все эти элементы.

Приёмопередающая станция генерирует лазерный импульс с длиной волны 1550 нм, который после циркулятора поступает на 1-й порт ответвителя X-типа. После ответвителя формируются два идентичных импульса. Первый импульс с 3-го порта ответвителя на пути к ВОПО меняет поляризацию на ортогональную исходной. В то время как 2-й импульс с 2-го порта ответвителя проходит через ВОЛЗ_Б и ВОФМ_Б на 2-й порт ВОПО. Причём за счёт ВОЛЗ_Б 2-й импульс задерживается на 50 нс относительно 1-го импульса. С 3-го порта ВОПО в ВОЛС

поступают два ортогонально поляризованных импульса с временной задержкой относительно друг друга.

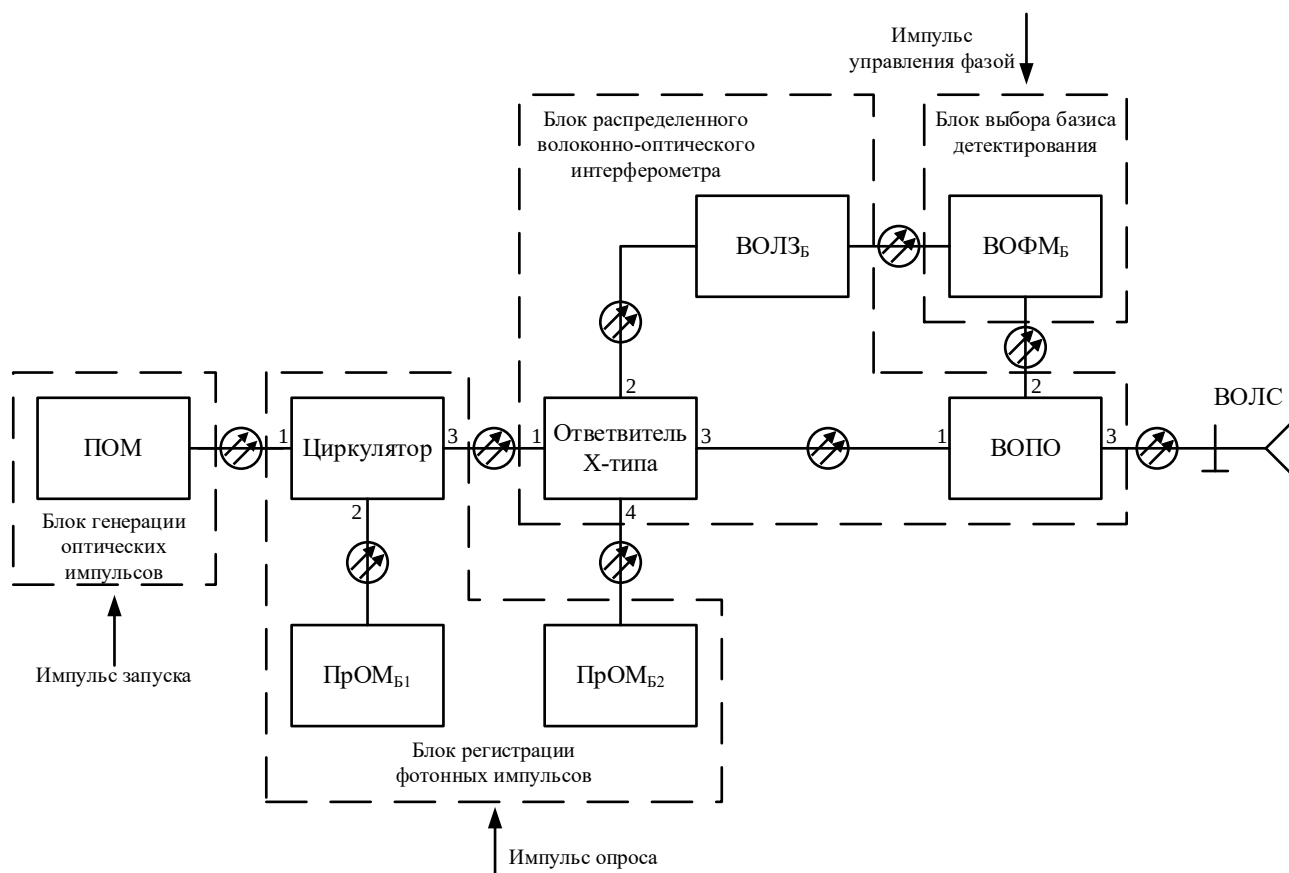


Рисунок 1.2 – Структурная схема приёмопередающей станции системы id 3000 Clavis

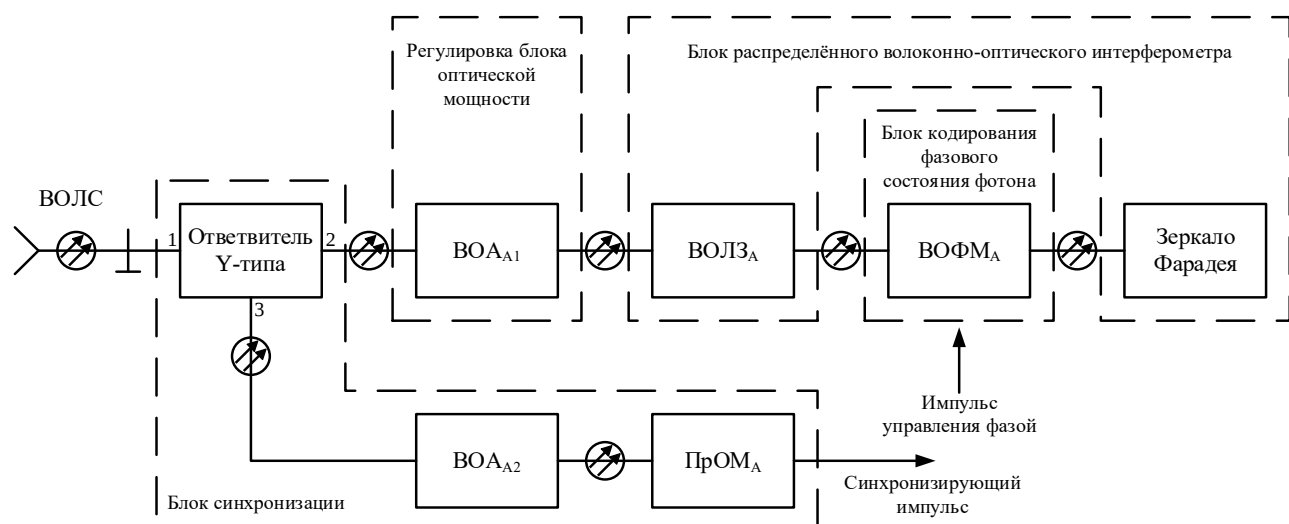


Рисунок 1.3 – Структурная схема кодирующей станции системы id 3000 Clavis

После распространения через ВОЛС импульсы попадают в кодирующую станцию, где отражаются от зеркала Фарадея, следовательно, становятся

ортогонально поляризованными не только относительно друг друга, но и относительно состояний на выходе приёмопередающей станции. На обратном пути импульсы ослабляются ВОА. На входе в приёмопередающую станцию вследствие изменения поляризации в кодирующей станции 1-й и 2-й импульсы поступают на 2-й и 1-й порт ВОПО соответственно, тем самым проходя по оптическим путям, противоположным при прямом прохождении в станции. Далее импульсы интерферируют в ответвителе X-типа и регистрируются 1-м или 2-м ПрОМ.

Рисунок 1.4 иллюстрирует применение системы Clavis-300 Quantum Cryptography Platform в конфигурации точка-точка (рисунок 1.4, а) или в качестве ретрансляционного узла для распределения ключей на большие расстояния (рисунок 1.4, б) [60].

Сейчас компания ID Quantique предоставляет системы КРК Cerberis-3 QKD System [61], Clavis-3 QKD Platform [62], Clavis-300 Quantum Cryptography Platform [60], Cerberis XG QKD System [63]. Модель Cerberis XGR QKD Platform [64] серии XG четвёртого поколения КРК выпущена в 2021 г [65]. Основные характеристики систем сведены в таблицу 1.1.

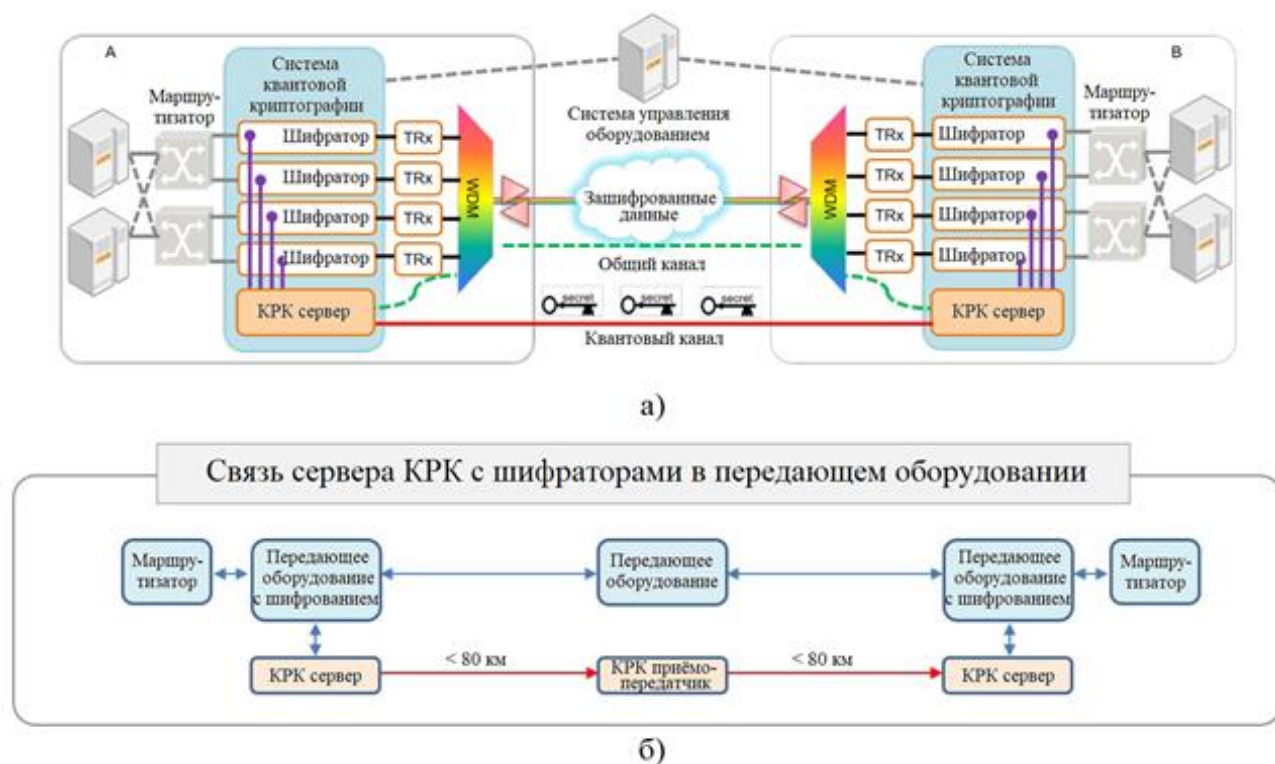


Рисунок 1.4 – Применение системы Clavis-300 в конфигурации точка-точка (а), в качестве ретрансляционного узла (б)

Таблица 1.1 – Основные характеристики систем КРК компании ID Quantique

Система КРК	Скорость генерации ключа	Дальность передачи ключа, км
Clavis XG QKD System	>100 Кбит/с	до 150
Cerberis XG QKD System	2 Кб/с	до 90
Cerberis-3 QKD System	1,4 Кб/с	80
Clavis-3 QKD Platform	1,4 Кб/с	75
Clavis-300 Quantum Cryptography Platform	10 Кб/с	70

Компания ID Quantique также разработала системы сетевой безопасности Centauris CN9000 Series [66], Centauris CN6000 Series [67], Centauris CN4000 Series [68] и Centauris CV1000 Virtual Encryptor [69]. Данные системы обеспечивают высокий уровень безопасности данных путём использования потокового шифрования с применением квантовых ключей.

Компания MagiQ (США) предлагает системы QPN 5505 [70], QPN7505 [71] и QPN 8505 [72], которые обеспечивают расширенную сетевую безопасность и надежную защиту от проблем с распределением ключей и управлением.

На рисунке 1.5 представлена архитектура сети КРК с двумя компьютерами с использованием системы MagiQ QPN 5505 [70]. В отличие от системы id 3000 Clavis, приёмопередающая станция системы MagiQ QPN 5505 содержит ВОА, через который проходят генерируемые ПОМ лазерные импульсы, претерпевая ослабление до заданного уровня. Приёмопередающая станция (Боб) и кодирующая станция (Алиса) соединены двумя каналами. Квантовый канал используется непосредственно для КРК, а канал синхронизации обеспечивает синхронизацию станций для корректного и эффективного функционирования системы в целом. Необходимо отметить, канал синхронизации состоит из информационного подканала и подканала синхронизации, объединённых волновым мультиплексором. Станции включают ряд служб, необходимых для КРК. Служба SNMP производит мониторинг управления сетью клиентов, использующей протокол SNMP. Служба QPN выполняет КРК, калибровку и диагностику системы, функции обслуживания системы. Служба Key Manager отправляет ключи шифрования с QPN модуля в приложение Encryption Bridge и, при наличии, в другие приложения шифрования, включая внутренние приложения. Служба

Encryption Bridge предоставляет клиентам услугу безопасного туннелирования данными путём шифрования и пересылки клиентских пакетов с открытым текстом между приёмопередающей и кодирующей станциями.

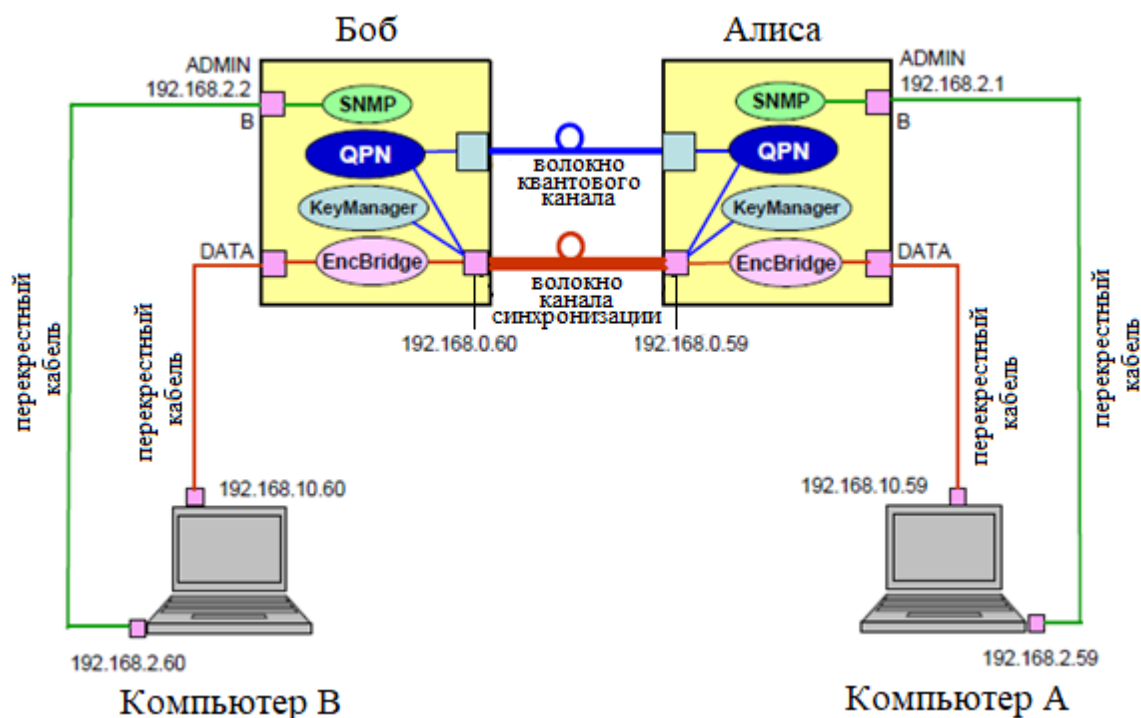


Рисунок 1.5 – Архитектура сети КРК с системой MagiQ QPN 5505

Системы id 3000 Clavis и MagiQ QPN 5505 работают по принципу «plug&play». В системе id 3000 Clavis линия синхронизации и КРК объединены в один канал. В аппаратуре MagiQ QPN 5505 синхронизация обеспечивается дополнительными линией коммуникации и приёмопередающим модулем.

Функционирование рассмотренных систем КРК основано на принципе автокомпенсационной схемы с фазовым кодированием состояний фотонов. В [32] рассмотрено функционирование волоконно-оптических автокомпенсационных систем КРК с фазовым кодированием состояний фотонов. На рисунке 1.6 представлена структура системы КРК с фазовым кодированием состояний фотонов, функционирующая по принципу «plug&play» [30].

При распространении по квантовому каналу фотоны претерпевают случайные изменения поляризации, вызванные воздействиями внешней среды и двойного лучепреломления в ОВ [73, 74, 75, 76]. Системы, функционирующие по принципу «plug&play», автоматически компенсируют поляризационные искажения [1, 51]. Автокомпенсационные системы упрощают процесс

формирования и распределения ключа, т.к. для их функционирования достаточно только наличия синхронизации станций. Зеркало Фарадея и волоконно-оптический интерферометр обеспечивают отсутствие двулучепреломления, следовательно, нет необходимости регулировки поляризации на обеих станциях. Также отличительной особенностью автокомпенсационных систем КРК является устойчивость работы при изменениях внешних условий [77].

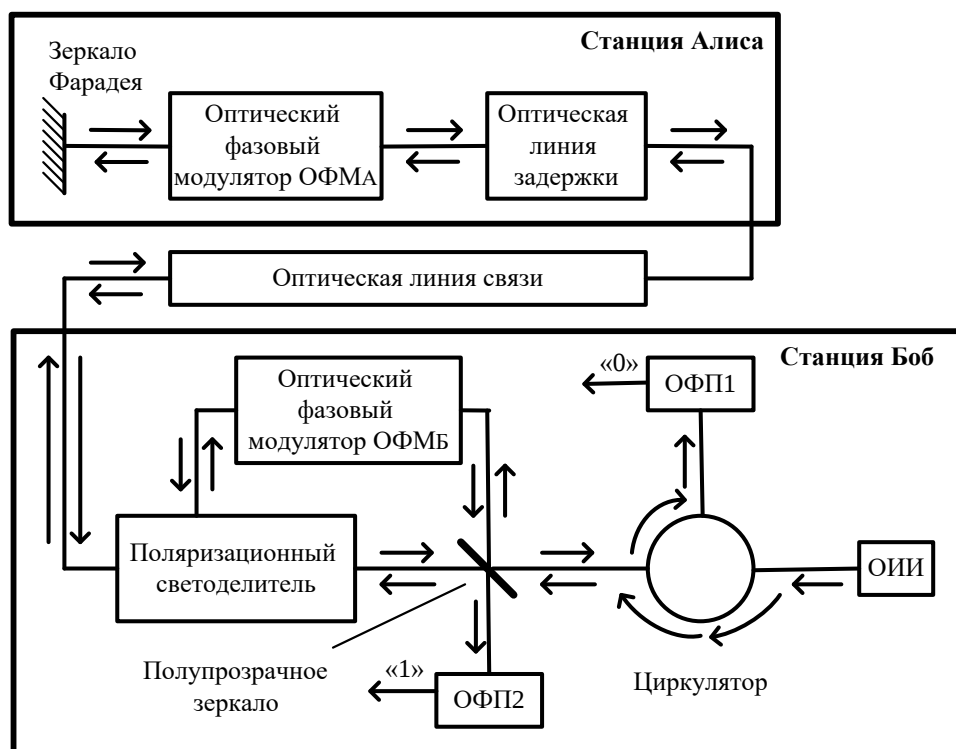


Рисунок 1.6 – Структурная схема системы КРК с фазовым кодированием состояний фотонов и автоматической компенсацией искажений поляризации

Резюме. Проанализированы автокомпенсационные системы КРК с фазовым кодированием состояний фотонов. Системы отличаются стабильной и устойчивой работой, поэтому они взяты за основу для последующего анализа. Определена типовая структура автокомпенсационной системы КРК, которая реализует выбранный протокол BB84, отличающийся значительной протяжённостью передачи секретного ключа. В процессе анализа установлено, что в структуру всех рассмотренных систем КРК включены подсистемы синхронизации, которые определяют качество КРК.

1.3 Исследование процесса синхронизации квантовых систем связи

Перед КРК проводится синхронизация станций. Синхронизация станций обеспечивается специальной подсистемой синхронизации и гарантирует

стабильную и устойчивую работу системы в целом. Для достижения высокой эффективности необходимо точно знать границы временного интервала, характерного для бита [10].

В радиосистемах хорошо изучено влияние гауссовских шумов на синхронизацию [12]. Однако системы КРК кардинально отличаются от традиционных систем, например, в системах КРК иная модель выходного сигнала фотодетектора. В системах КРК в выходном токе необходимо учитывать квантовую составляющую шума, связанную с наличием полезного сигнала.

Рассмотрим случай организации КРК и синхронизации по двум разным каналам, причём канал синхронизации включает линию для синхронизации станций и линию для передачи информационных данных путём частотного или временного мультиплексирования.

На рисунке 1.7 представлена упрощённая структура приёмной станции с подсистемой синхронизации. Синхронизирующая информация в общем случае поступает на вход подсистемы синхронизации в виде синхронизирующих сигналов (далее синхросигналов) или сигналов временных меток.

При частотном мультиплексировании синхросигналы в передатчике, генерирующем оптическое излучение на фиксированной длине волны, «накладываются» на информационные потоки (занимают неперекрывающиеся области частотного спектра). Такой комбинированный сигнал излучается в канал и поступает на вход приёмной станции. Выделяемый приёмным оптическим модулем сигнал подаётся на вход электронного демультиплексора, в котором происходит разделение информационных сигналов и синхросигналов. Таким образом, процесс синхронизации работает параллельно с приёмом информационного сигнала.

При временном разделении синхросигналы посылаются в течение одного временного интервала, а информационные потоки – в других интервалах. В обоих случаях разделения подсистема синхронизации выделяет синхросигнал либо с помощью временного стробирования, либо с помощью частотной фильтрации.

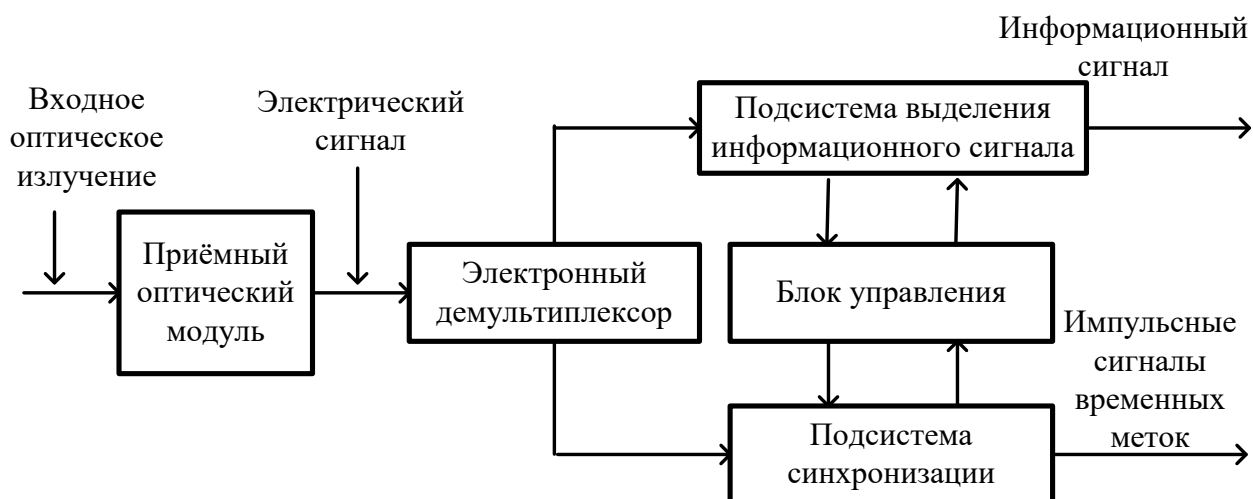


Рисунок 1.7 – Упрощённая структура приёмной станции с подсистемой синхронизации

Рассмотрим временную синхронизацию. Под «чистой» синхронизацией будем понимать отсутствие влияния синхросигнала на информационный сигнал в процессе разделения комбинированного сигнала. Для процедуры синхронизации необходимо определить моменты прихода указанных импульсов, которые в то же время являются временными маркерами.

Проблему синхронизации станций можно определить как проблему оценки момента прихода синхросигнала, решение которой подразделяется на два этапа. Первый этап именуется «грубой» оценкой момента приёма синхросигнала и заключается в дискретизации выделенного временного отрезка, равного по длительности периоду следования синхросигнала, на временные интервалы и нахождении интервала с оптическим импульсом. Второй этап именуется «точной» оценкой и заключается в уточнении временного сдвига внутри найденного интервала (рисунок 1.8). В [10] показано, что граница Крамера-Рао для оценки момента приёма синхросигнала минимальна, если передаётся периодическая последовательность прямоугольных коротких импульсов. Такая реализация интенсивности фотонов и ИТТ соответствует передаче узких оптических синхроимпульсов. Поэтому периодическая последовательность узких оптических импульсов – наиболее подходящая форма синхросигнала.

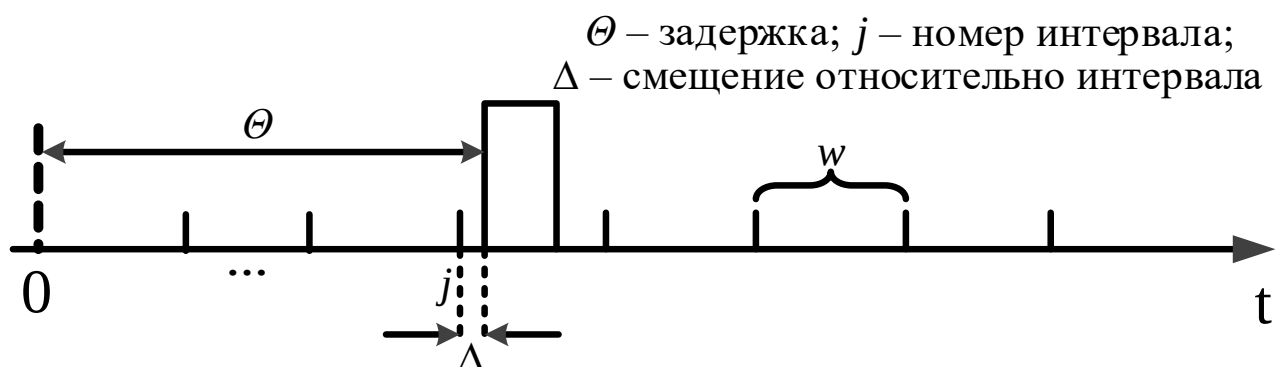


Рисунок 1.8 – Модель процесса поступления оптического импульса

После установления синхронизации станций необходимо её поддерживать вследствие наличия помех и шумов как в системе, так и внешних. Для поддержания синхронизации используется операция слежения (рисунок 1.9).

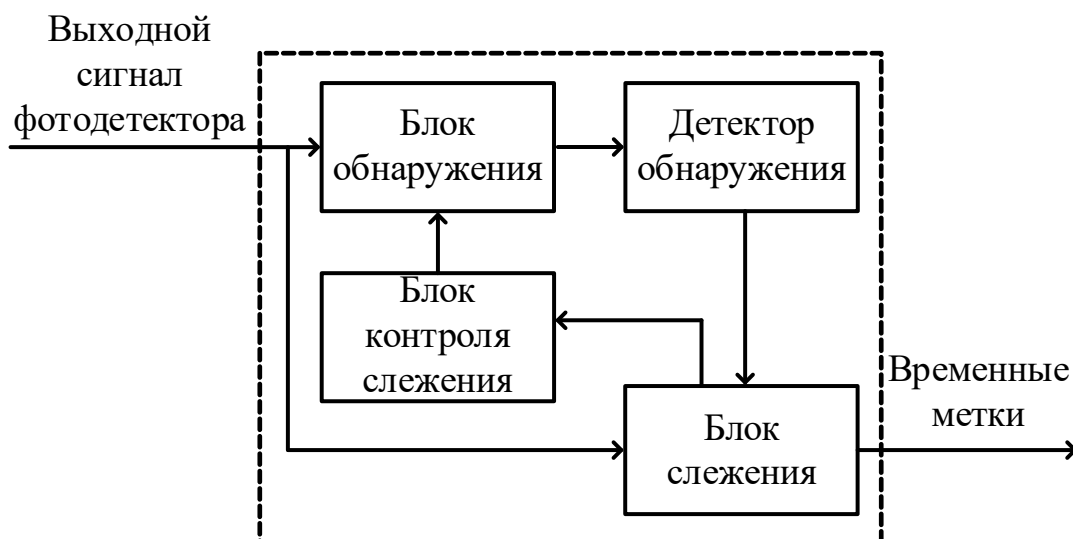


Рисунок 1.9 – Элементы подсистемы синхронизации

Возникающие временные сдвиги достаточно малы, поэтому данная операция функционально проще операции синхронизации. Операция слежения выполняется на протяжении всего сеанса связи. При сбое операции слежения необходимо заново провести операцию синхронизации.

Испытания систем id 3110 Clavis 2 [78] и QPN 5505 [79] показали, что процесс синхронизации реализуется в многофотонном (токовом) режиме, что упрощает злоумышленнику организацию несанкционированного доступа к информации или внесения помех. Также потенциально упрощается НСД к информации или внесение помех из-за технического несовершенства оптоэлектронных компонентов

синхронизации [4]. Для этого злоумышленник должен получить информацию о времени опроса оптических детекторов [8, 9].

Известен патент на способ синхронизации передатчика и приёмника в двухпроходной автокомпенсационной системе КРК [80], обеспечивающий усиление защищённости процесса синхронизации передатчика и приёмника. Способ обеспечивает связь посредством квантового канала между станциями; генерирование опорного сигнала на одной из станций; передачу сгенерированного опорного сигнала через опорный канал на другую станцию; использование опорного сигнала для синхронизации электрических сигналов в квантовой системе.

Способ включает отправку сигналов синхронизации с первой станции на вторую станцию по отдельному каналу синхронизации и запись данных о времени прихода синхросигналов на вторую станцию. В пределах одной станции опорный сигнал используется блоком управления для синхронизации блока опорных сигналов в другой станции. Блоки управления временными процессами находятся на каждой станции. Причём один блок выполняет функцию ведущего, а второй – ведомого блока. Ведомый блок управления синхронизируется с ведущим на основании информации, передаваемой по каналу от блока управления.

Повышение безопасности КРК достигается селекцией синхросигналов от сигналов, которые не принадлежат переданным синхросигналам первой станцией по каналу синхронизации. Если обнаружено, что дополнительные сигналы в канале синхронизации могут быть вызваны атакой на систему, генерируется сигнал тревоги. Кроме того, усиление защищённости канала синхронизации достигается путём контроля времени стробирования фотодетекторов.

Недостатком способа является использование отдельной среды распространения для синхронизации станций и передачи квантовых сигналов. Причём способ подразумевает контроль процесса за счёт стробирования, что может значительно увеличить время синхронизации. Кроме того, в способе нет упоминания об уровне сигнала синхронизации, т.е. принимается линейный режим синхронизации, который предполагает наличие мощного синхроимпульса.

Известен патент на способ [81], обеспечивающий двусторонний обмен квантовыми сигналами, сигналами синхронизации и данными общего пользования. Система содержит первые приёмопередатчик для передачи и приёма данных, оптический модулятор/демодулятор для обмена сигналами синхронизации, квантовый приёмопередатчик для обмена квантовыми сигналами и регулятор, связанный с первыми приёмопередатчиком данных, оптическим модулятором/демодулятором и квантовым приёмопередатчиком. Первый регулятор способен к управлению передачей данных, сигналов синхронизации и квантовых сигналов.

Один из вариантов реализации способа предполагает следующую последовательность шагов: передача данных в первом кадре синхронизации; прекращение передачи данных в течение периода; передача квантовых сигналов и сигналов синхронизации в течение следующего кадра синхронизации. Для этого система обеспечивает временное мультиплексирование в одно оптоволокно квантовых сигналов, сигналов синхронизации и данных. Причём квантовые сигналы и сигналы синхронизации передаются в одно и то же время, а данные общего пользования – в другое время.

Недостатком способа является использование для синхронизации станций мощных оптических импульсов. Причём предполагается передача данных в первом кадре синхронизации; прекращение передачи данных в течение периода; передача квантовых сигналов и сигналов синхронизации в течение следующего кадра синхронизации. Естественно, что посылка в канал связи синхронизирующих лазерных импульсов в многофотонном режиме упрощает НСД и съём синхросигналов. Кроме того, описывается ситуация уточнения привязки по времени квантовых состояний на станциях. Однако вопрос о первоначальной синхронизации в момент запуска системы КРК не раскрыт.

Резюме. Синхронизация станций системы КРК является одной из важнейших процедур для обеспечения эффективного и стабильного функционирования системы в целом. Существующие методы синхронизации предусматривают использование мощных (многофотонных) сигналов, что значительно упрощает

НСД, съём данных и внесение помех в канал передачи. Поэтому актуален поиск новых методов синхронизации, которые будут гарантировать более высокую безопасность.

1.4 Специфика однофотонной синхронизации станций квантового распределения ключа

Важнейшей составляющей эффективной работы системы КРК является синхронизация разнесённых в пространстве станций посредством периодической последовательности оптических синхроимпульсов. Вопросы безопасности систем КРК и синхронизации станций изучались в работах отечественных и зарубежных учёных [42, 82, 83, 84, 85, 86, 87, 88, 89].

Одно из направлений повышения защищённости процесса вхождения в синхронизм от НСД – использование однофотонной синхронизации станций в автокомпенсационной системе КРК. Однофотонная синхронизация активно развивалась группой учёных во главе с Румянцевым К.Е. [23, 90, 91, 92]. Здесь в качестве синхросигналов используются фотонные импульсы [14, 15], которые представляют ослабленные импульсы ПОМ. Отметим, что ослабление оптического импульса до фотонного уровня (в среднем менее одного фотона на импульс) обеспечивается при обратном распространении синхросигнала по ВОЛС от кодирующей станции к приёмопередающей [83, 93].

В процессе синхронизации выделяются временные кадры с длительностью, равной периоду следования фотонных импульсов T_s . Каждый кадр разбивается на конечное число временных окон с фиксированной длительностью τ_w . Окна с одинаковыми порядковыми номерами внутри кадров соответствует анализу одних и тех же участков ВОЛС.

В [93, 94] положение временного окна, в котором находится синхроимпульс, определяется с помощью подсчёта импульсов с выхода однофотонного фотодетектора в каждом окне. Отметим, что в число подсчитанных импульсов могут входить не только отклики фотодетектора на приём фотона, но и шумовые (помеховые) ИТТ.

В [10] положение временных окон, в которых может находиться синхроимпульс, определяется с помощью анализа пары смежных окон. Такой алгоритм обнаружения синхроимпульса учитывает принадлежность фотонного импульса сразу паре окон. Программа испытаний продолжается до тех пор, пока не будет превышен пороговый уровень. Другая возможная программа поиска состоит в накоплении отсчётов в окнах, соответствующих одним и тем же участкам ВОЛС, и выделении пары смежных окон с максимальной суммой отсчётов. При этом считается, что первый этап синхронизации завершён. Аппаратура переходит ко второму этапу уточнения временного местоположения синхроимпульса.

Описанные в [95] алгоритмы синхронизации предусматривают накопление отсчётов в окнах временных кадров с одинаковыми порядковыми номерами и выделении окна (а не пары окон) с максимальной суммой отсчётов. Справедливость подхода вытекает из того, что на первом этапе синхронизации время анализа окна во много раз больше длительности синхроимпульса.

Указанные алгоритмы синхронизации для обеспечения энергетической скрытности процесса синхронизации используют однофотонную передачу, что накладывает значительные ограничения на дальность ВОЛС. Поэтому исследования однофотонной синхронизации с целью увеличения дальности ВОЛС при сохранении повышенной защищённости от НСД [91, 96] являются актуальной проблемой.

Алгоритм в [97, 98] не предполагает разбиение временных кадров на окна и накопление отсчётов с каждого участка ВОЛС. Аппаратура изначально работает в режиме поиска фотона. При первом превышении порогового уровня процессом с выхода однофотонного фотодетектора аппаратура переходит в режим тестирования. Повторный опрос фотодетектора производится только в интервалах ожидаемого прихода фотона, определяемого импульсом стробирования длительностью τ_{strob} . В остальное время канал не реагирует на приём фотонов.

Сравнительный анализ временных характеристик показывает, что двухэтапный алгоритм синхронизации обеспечивает значительный выигрыш (в сотни раз) во времени вхождения в синхронизм в коротких ВОЛС при

использовании реального однофотонного лавинного фотодиода (ОЛФД), по сравнению с ранее описанным алгоритмом [99]. Установлено, что для двухэтапного алгоритма синхронизации возможно применение ОЛФД со значительной временной задержкой между моментами приёма фотона, образования лавины, её гашения и последующего восстановления работоспособности фотодетектора.

Анализ двухэтапного алгоритма синхронизации [90] показывает, что, увеличивая количество тестов, можно сделать вероятность ошибки тестирования сколь угодно малой. Однако добиться сколь угодно близкой к 1 вероятности обнаружения фотонного импульса на этапе поиска, увеличивая число кадров (время анализа), невозможно. Следовательно, нельзя при значительной протяжённости ВОЛС получить сколь угодно малую вероятность ошибки синхронизации. Этот фактор ограничивает дальность КРК.

В связи с этим поиск нового алгоритма однофотонной синхронизации, свободного от указанных недостатков, является актуальной задачей.

Резюме. Применение однофотонной синхронизации станций повышает защищённость передаваемых данных. Существующие методы предполагают значительные временные затраты или ограниченную протяжённость ВОЛС. Следовательно, является актуальным исследование однофотонной синхронизации станций автокомпенсационной системы КРК на однофотонных ЛФД при сохранении защищённости от НСД.

1.5 Постановка общей научной задачи и формулировка частных задач диссертационных исследований

Теоретически абсолютная секретность передачи информации может быть реализована с помощью только протоколов квантовой криптографии. Проведён анализ протоколов квантовой криптографии, среди которых выделен протокол BB84, отличающийся значительной протяжённостью передачи секретного ключа наряду с обеспечением его безопасности.

Проведён анализ автокомпенсационных систем КРК с фазовым кодированием состояний фотонов по протоколу BB84, ключевой особенностью

которых является стабильность и устойчивая работа. Доказано, что для корректного и эффективного функционирования необходима синхронизация приёмопередающей и кодирующей станций.

Анализ подсистем синхронизации коммерческих решений систем КРК показывает уязвимость последних к НСД ввиду функционирования в многофотонном режиме. Поэтому поиск новых алгоритмов синхронизации станций системы КРК с обеспечением повышенной безопасности является актуальной проблемой.

Для обеспечения скрытности процесса синхронизации волоконно-оптической системы КРК с автоматической компенсацией поляризационных искажений предложено использовать фотонные синхроимпульсы, представляющие оптический импульсы, ослабленные до уровня регистрации в них в среднем менее одного фотона. Применение фотонных импульсов значительно затрудняет использование части энергии синхроимпульса злоумышленником для синхронизации своей аппаратуры, что гарантирует повышенную защищённость процесса синхронизации.

Анализ двухэтапного временного метода показывает его высокую эффективность при протяжённости ВОЛС в 10...20 км. К сожалению, при протяжённости ВОЛС более 20 км, когда среднее число ИТТ за длительность временного кадра становится соизмеримо со средним число фотонов в фотонном импульсе, метод не применим.

Существующие методы синхронизации станций волоконно-оптической системы КРК, предполагая значительные временные затраты, не гарантируют скрытности процесса синхронизации. Использование однофотонного режима синхронизации, где применение ослабленного до квантового уровня излучения затрудняет НСД к информации, предполагает значительные временные затраты и ограниченную протяжённость ВОЛС. Актуальной проблемой является поиск алгоритма синхронизации станций автокомпенсационной системы КРК на однофотонных ЛФД, гарантирующего протяжённую ВОЛС при сохранении энергетической скрытности синхронизации.

Цель диссертационных исследований: увеличение протяжённости ВОЛС в автокомпенсационной системе КРК на однофотонных ЛФД при сохранении энергетической скрытности синхронизации на основе протокола BB84.

Объект исследований: автокомпенсационная система КРК по оптическому волокну на основе протокола BB84.

Предмет исследований: алгоритм двухэтапной синхронизации автокомпенсационной системы КРК в однофотонном режиме.

Общая научная задача: разработка и исследование алгоритма вхождения в синхронизм автокомпенсационной системы на однофотонных ЛФД, гарантирующего протяжённую ВОЛС при сохранении энергетической скрытности синхронизации и обеспечении вероятности ошибки синхронизации не выше требуемого значения. Создание методик расчёта и основ проектирования подсистем синхронизации, защищённых от НСД.

Частные задачи диссертационных исследований:

– анализ подсистем синхронизации станций автокомпенсационных систем КРК в существующих коммерческих решениях. Обоснование актуальности, определение общей научной задачи и частных задач исследований;

– синтез алгоритма синхронизации станций автокомпенсационной системы КРК с повышенной защитой от НСД, обусловленной применением однофотонного уровня передачи, и двухэтапным определением момента появления фотонного импульса;

– определение аналитических выражений для расчёта энергетических, вероятностных и временных параметров алгоритма синхронизации станций автокомпенсационной системы КРК;

– моделирование процесса синхронизации автокомпенсационной системы КРК для доказательства эффективности разрабатываемого алгоритма.

2. РАЗРАБОТКА ДВУХЭТАПНОГО АЛГОРИТМА СИНХРОНИЗАЦИИ С РАЗБИЕНИЕМ ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ НА УЧАСТКИ С УБЫВАЮЩЕЙ ДЛИНОЙ

2.1 Сравнительный анализ технических решений аппаратуры синхронизации

Проведём анализ существующих подсистем синхронизации станций.

Известен способ синхронизации [80] для повышения безопасности системы КРК, представленной на рисунке 2.1. Система включает передающую и приёмную станции, соединённые ВОЛС. Передающая станция (Боб) включает ПОМ 20 для генерации двух когерентных оптических импульсов P_1 и P_2 . Модуль 20 состоит из оптического фазового модулятора (ΦM_B), лазерного источника (ЛИ) и регулируемого аттенюатора (PA_B). Модулятор ΦM_B соединён с контроллером напряжения (KH_B), который связан с генератором случайных чисел ($ГСЧ_B$). $ГСЧ_B$ соединён с контроллером (K_B), который, в свою очередь, связан с оптическим модулем 20 через блок однофотонных фотодетекторов 40. Блок 40 состоит из двух однофотонных детекторов ($ОФД_1$ и $ОФД_2$) и находится под управлением контроллера K_B .

Приёмная станция (Алиса) включает оптический фазовый модулятор (ΦM_A), зеркало Фарадея (ЗФ), регулируемый оптический аттенюатор (PA_A), контроллер напряжения (KH_A), генератор случайных чисел ($ГСЧ_A$) и контроллер (K_A).

Контроллеры K_B и K_A соответственно связаны оптически/электронно через канал синхронизации КС посредством синхросигналов СС. Контроллеры управляют работой оптических фазовых модуляторов ΦM_B и ΦM_A . В канале синхронизации также показан паразитный сигнал ПС, возникающий из-за шума в канале или в результате атаки на канал синхронизации.

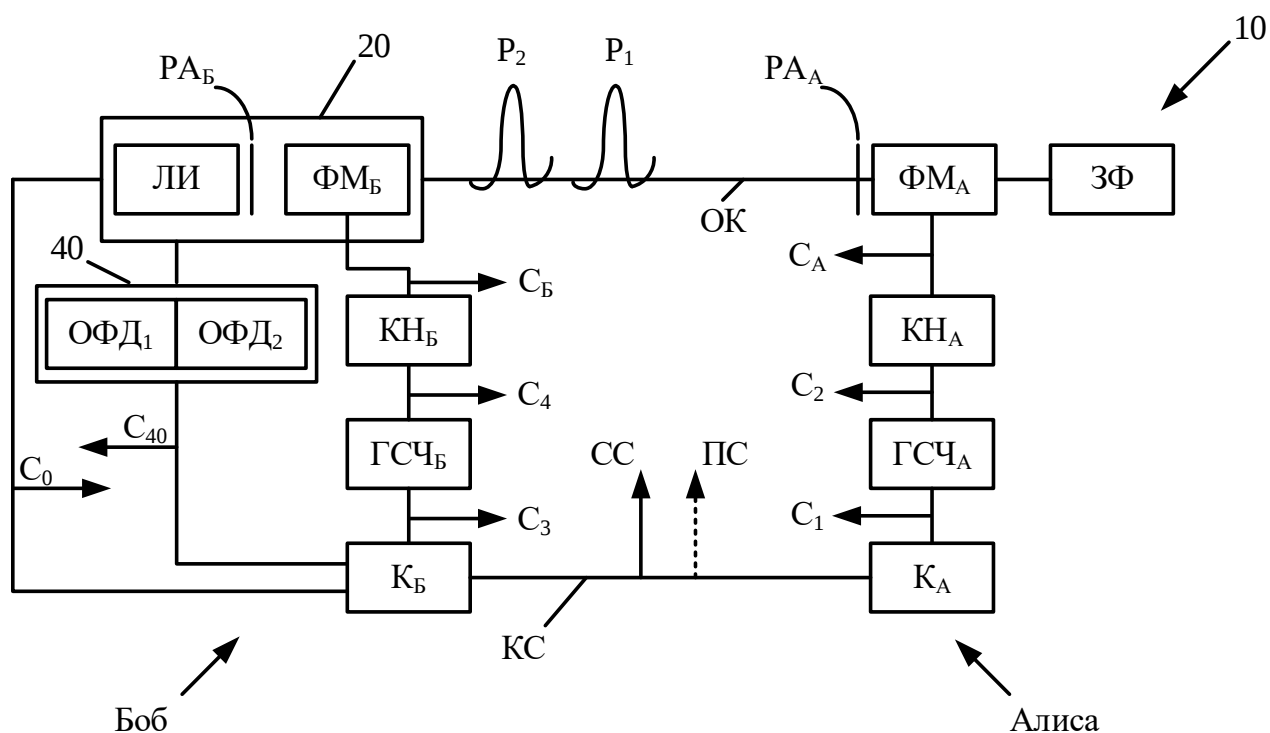


Рисунок 2.1 – Двусторонняя система КРК по патенту US7436961

Передача квантовых сигналов и сигналов синхронизации осуществляется по двум каналам – оптоволоконному каналу (ОК) и КС (рисунок 2.1). Контроллер K_B активирует ПОМ с помощью сигнала активации (C_0) для генерации когерентных оптических импульсов P_1 и P_2 , имеющих ортогональные поляризации. Импульсы проходят через модулятор ΦM_B в выключенном состоянии и через регулируемый аттенюатор PA_B . Затем импульсы передаются Алисе по каналу ОК. Затем импульсы P_1 и P_2 проходят через модулятор ΦM_A в выключенном состоянии. Фотоны, отражённые от зеркала Фарадея, изменяют поляризацию на 90° . Когда импульсы проходят обратно через модулятор ΦM_A , станция, пропуская первый импульс P_1 без модуляции, модулирует фазу второго импульса P_2 . Фаза импульса P_2 задаётся контроллером K_A , подающим сигнал C_1 на генератор $ГСЧ_A$, который генерирует случайное число C_2 на контроллер напряжения $КН_A$. Контроллер $КН_A$ отправляет случайно выбранный сигнал C_A управления в модулятор ΦM_A , чтобы установить фазовый сдвиг $+3\pi/4$, $-3\pi/4$, $+\pi/4$ или $-\pi/4$.

Два импульса P_1 и P_2 проходят через аттенюатор PA_A , который формирует фотонные импульсы. Импульсы возвращаются к Бобу, причём импульс P_2 проходит без изменений через оптический модулятор ΦM_B , а импульс P_1 получает

случайный фазовый сдвиг. Фаза задаётся контроллером K_B , генерирующим сигнал C_3 на ГСЧ_Б, который выдаёт случайное число C_4 на контроллер КН_Б. В ответ контроллер КН_Б отправляет случайно выбранный сигнал C_B управления в модулятор ФМ_Б для установления фазового сдвига на $+\pi/4$ или $-\pi/4$.

Импульсы P1 и P2 интерферируют в оптическом модуле 20. Результирующий импульс направляется в блок однофотонных детекторов 40. Фотонный импульс с разностью фаз равной 0 поступает на фотодетектор ОФД₁ (регистрация бита «0»), а с разностью фаз π на фотодетектор ОФД₂ (регистрация бита «1»).

Если базис фазы Боба отличается от базиса Алисы, результирующий импульс поступает в любой из двух ОФД с равной вероятностью, а результат измерения считается неопределённым. Регистрируемый сигнал в блоке однофотонных детекторов 40 передаётся в контроллер K_B (формируется сигнал C_{40}), где состояния фазы сохраняются вместе с состояниями модуляции, переданными в модулятор ФМ_Б.

На рисунке 2.2 представлена временная диаграмма, показывающая синхросигналы с интервалами стробирования и паразитные сигналы.

Рабочий цикл синхронизации порядка 0,5% от общего времени означает, что время на съём информации о фазовом состоянии фотона очень мало. Действительно, ожидаемое время приёма синхроимпульса определяется временным окном синхросигнала (ВОС), которое составляет около $\pm 1\%$ от периода следования синхроимпульсов. Например, для частоты синхроимпульсов 1 МГц ширина окна составляет ~ 20 нс.

Как показано на рисунке 2.1, синхросигналы принимаются контроллером K_B , который синхронизирует работу модулятора ФМ_Б и стробирование фотодетекторов.

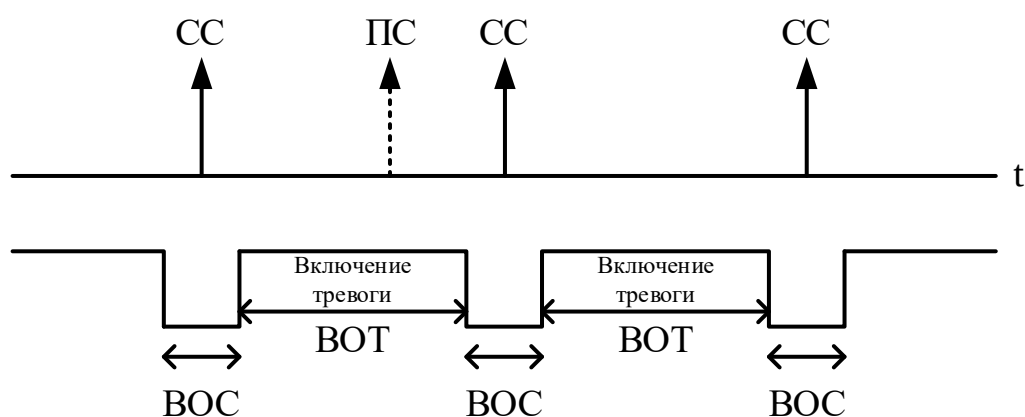


Рисунок 2.2 – Синхросигналы и паразитные импульсы в канале синхронизации

Контроллеры K_A и K_B формируют фазовые сдвиги модуляторов ΦM_A и ΦM_B в течение их стробирования.

Отметим, что канал синхронизации КС на рисунке 2.1 включает паразитный сигнал ПС, который может являться системным шумом или импульсом злоумышленника. Таким образом подчёркнуто, что канал синхронизации необходимо контролировать для гарантии безопасности системы. Любые несоответствующие импульсы или уровни напряжения, которые обнаруживаются в течение временного окна, интерпретируются как атака. Генерируется сигнал тревоги C_T для информирования пользователя о ситуации и принятия контрольных действий (например, завершение процесса обмена ключами).

Недостатком описанного способа является использование отдельной среды распространения квантовых сигналов и сигналов синхронизации. Также не отмечен уровень передаваемых сигналов синхронизации, поэтому принимается линейный режим синхронизации, предполагающий мощные синхроимпульсы, что значительно упрощает НСД к каналу синхронизации.

Известен способ синхронизации системы с КРК [100]. Система КРК включает передатчик и приёмник, соединённые ОВ. Передатчик принимает оптический импульсный сигнал и синхросигнал от приёмника и в соответствии с первым набором данных синхронизации генерирует передаваемый оптический импульсный сигнал с поляризацией отличной от поляризации исходного оптического импульсного сигнала, который по оптическому волокну поступает на

вход приёмника. В приёмнике сигнал детектируется в соответствии с вторым набором данных синхронизации.

Передатчик включает фазовый модулятор, модулирующий фазу оптического импульсного сигнала на основе первого набора данных синхронизации; зеркало Фарадея, которое поворачивает поляризацию на 90° .

Приёмник включает поляризационный светоделитель для разделения передаваемого оптического импульсного сигнала на две части; фазовый модулятор, который модулирует фазу первой части импульсного сигнала на основе второго набора данных синхронизации; оптический ответвитель, объединяющий фазомодулированную первую и вторую части сигнала; обнаружитель, детектирующий объединённый сигнал в соответствии с импульсом синхронизации. Фазомодулированная часть сигнала проходит длинный оптический путь между поляризационным светоделителем и фазовым модулятором, в то время как вторая часть сигнала проходит короткий оптический путь между поляризационным светоделителем и оптическим ответвителем.

Оптическое волокно, соединяющее передатчик и приёмник, включает квантовый и классический каналы. Приёмник генерирует синхросигнал, который посредством классического канала поступает в передатчик. Частота синхросигнала регулируется так, что количество тактов в классическом канале всегда является положительным постоянным числом.

Синхронизация передатчика и приёмника происходит в следующем порядке:

- установление тактовой синхронизации между передатчиком и приёмником;
- передача оптического импульсного сигнала от приёмника передатчику;
- генерация оптического сигнала путём изменения поляризации оптического импульсного сигнала и передача посредством оптического волокна приёмнику;
- обнаружение оптического импульсного сигнала путём детектирования объединённых частей сигнала.

Тактовая синхронизация осуществляется передачей оптического тактового сигнала от приёмника к передатчику через классический канал по оптическому

волокну; отражением оптического синхросигнала от передатчика к приёмнику через классический канал; управлением частотой оптического синхросигнала.

На рисунке 2.3 представлена структура системы КРК, которая состоит из передатчика (100 – Алиса), приёмника (200 – Боб). Приёмник включает подсистему синхронизации (300). Оптическое волокно (400) соединяет передатчик и приёмник. Секретные ключи генерируются посредством взаимодействия Алисы и Боба через квантовый канал (401). Отфильтрованный фильтром нижних частот (ФНЧ, 302) сигнал подаётся на генератор (301), управляемый напряжением, для управления выходным синхросигналом. Синхронизация между станциями установлена через ВОЛС, причём количество тактов синхросигнала постоянно.

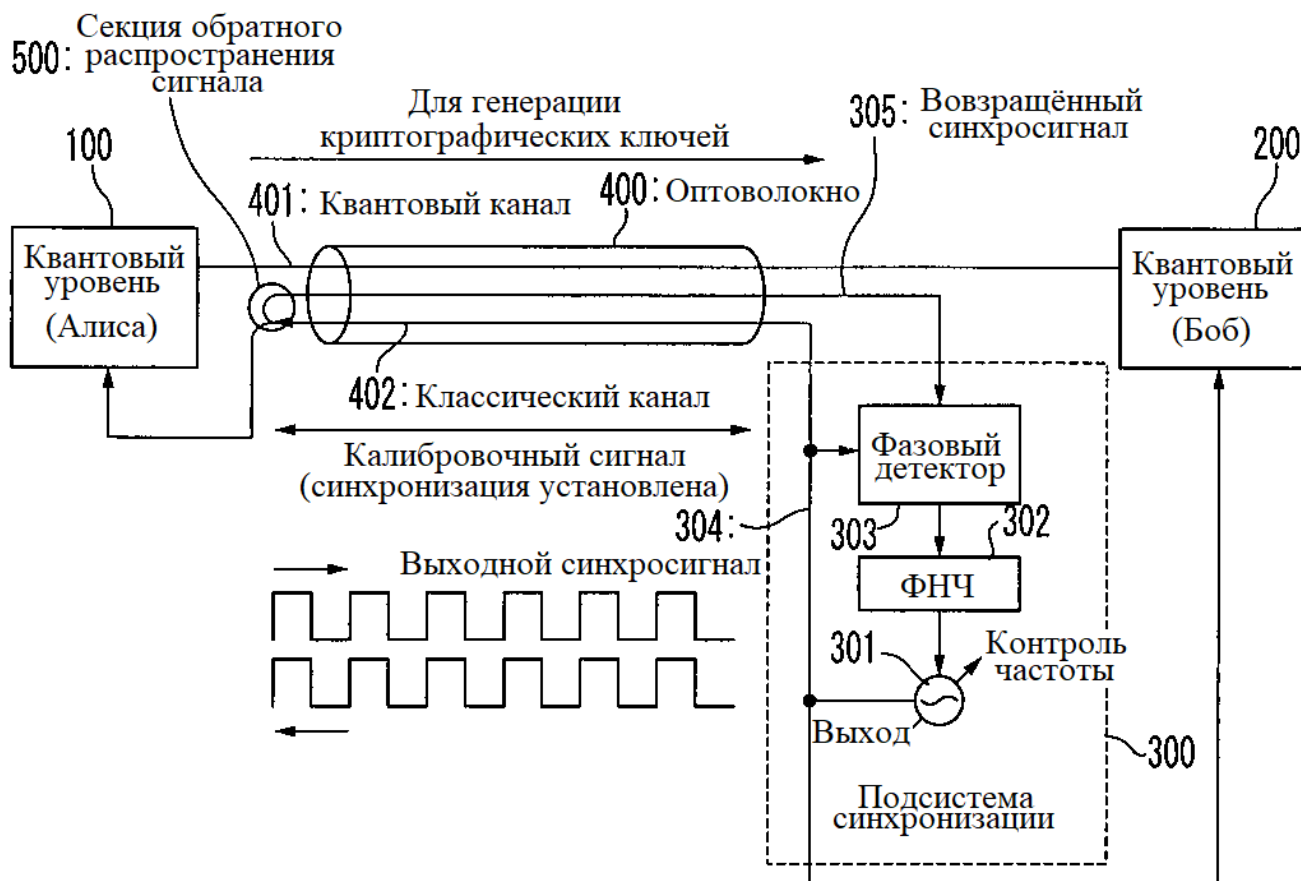


Рисунок 2.3 – Структура системы КРК по патенту US7869599 (1-й вариант)

На рисунке 2.4 представлена структура варианта системы КРК. Здесь квантовый канал (401) использует длину волны λ_1 , а классический канал (402), используемый для синхронизации, функционирует на длинах волн λ_2 и λ_3 . Алиса (100) и Боб (200) соединены оптическим волокном (400) посредством волновых мультиплексоров/демультиплексоров (601) и (602). Алиса включает фазовый

длинному путям. После прохождения плеч импульсы мультиплексируются. Далее объединённый импульс передаётся Алисе посредством мультиплексоров/демультиплексоров и ОВ. В это время блок настройки задержки настроен таким образом, что фазовый модулятор не выполняет операцию фазовой модуляции.

Поступившие мультиплексированные оптические импульсы в передатчик подаются на фазовый модулятор через аттенюатор. Фазовой модуляции подвергаются только те оптические импульсы, которые проходили по длинному пути в приёмнике. Сигнал начала работы фазового модулятора, пришедший из подсистемы синхронизации, синхронизируется с тактовым сигналом, который подаётся из секции возврата.

Зеркало Фарадея поворачивает фазы оптических импульсов на 90° . Отражённые от зеркала Фарадея оптические импульсы ослабляются аттенюатором до мощности, меньшей или равной одному фотону на бит. После ослабленные оптические импульсы снова возвращаются в приёмник.

В связи с поворотом фаз оптических импульсов на 90° , последние распространяются по путям, отличным от путей при прямом прохождении. Таким образом, теперь вторые части импульсов претерпевают фазовую модуляцию. Так как в сумме длины путей при прямом и обратном прохождении частей импульсов равны, то импульсы поступают на оптический делитель одновременно. Если разность фаз поступивших одновременно оптических импульсов равна 0, то оптические импульсы поступают на первый ЛФД. Если разность фаз между импульсами равна π , то они поступают на второй ЛФД. При разности фаз $\pi/2$ или $3\pi/2$ оптические импульсы с равной вероятностью поступают на один из двух ЛФД и считаются неопределёнными.

На рисунке 2.5 представлена структура системы КРК, отличающаяся от системы на рисунке 2.3 тем, что на станции Алиса добавлены делитель частоты $(1/N)$ 20 и генератор 11 ключей, а на станции Боб добавлен другой генератор 12 ключей.

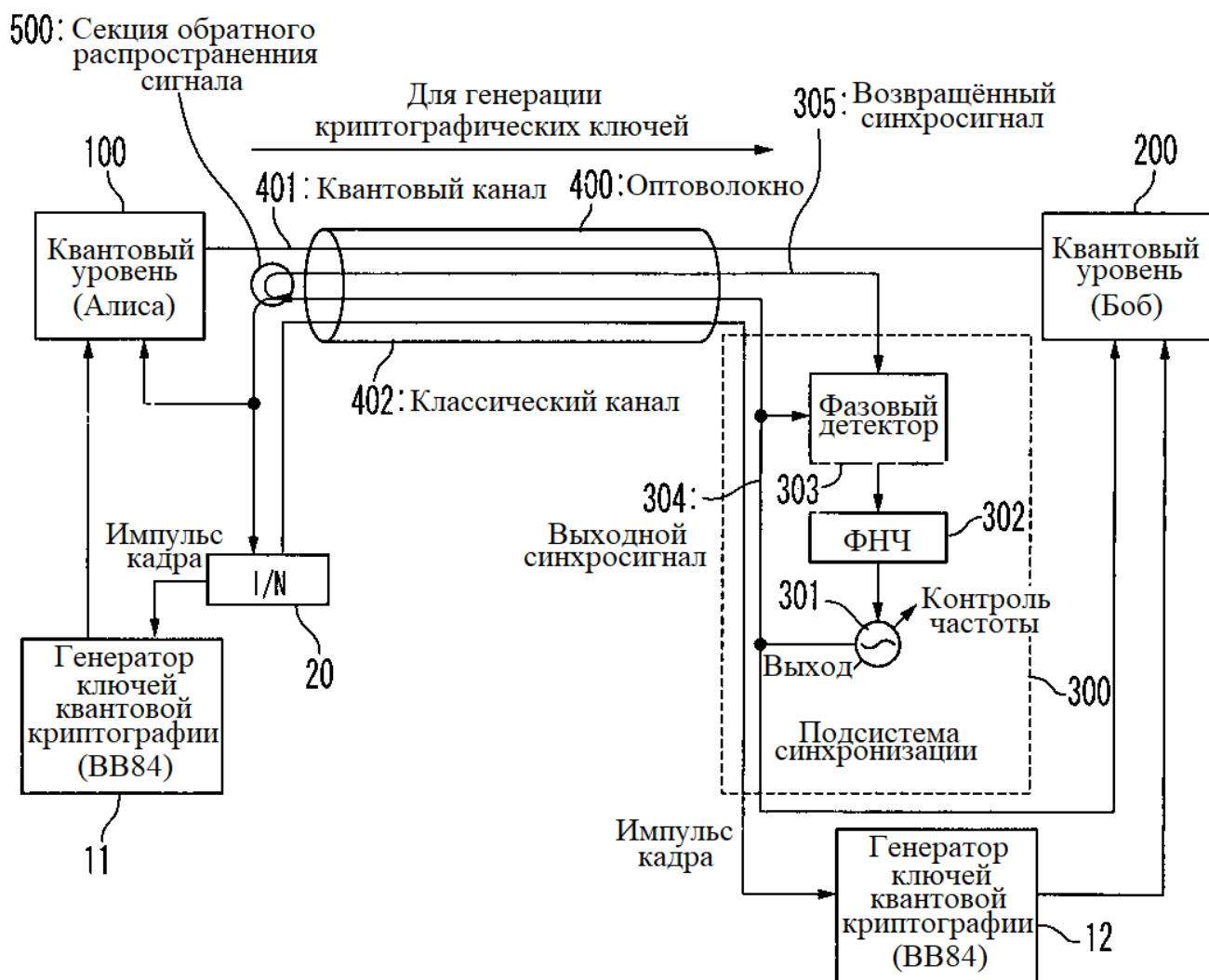


Рисунок 2.5 – Структура системы КРК по патенту US7869599 (3-й вариант)

В системе устанавливается не только тактовая, но и кадровая синхронизация. Кадровая синхронизация требуется для сопоставления битов, подлежащих сравнению друг с другом. Кроме того, в третьем варианте тактовый сигнал делится по частоте делителем 20 Алисы для генерации импульса кадра.

К недостаткам рассмотренных систем КРК можно отнести отдельные среды распространения квантовых и синхронизирующих сигналов. Причём отсутствует упоминание о возможной протяжённости канала связи, что ограничивает применение рассмотренных систем при значительных протяжёностях линии связи.

Аппаратура управления синхронизации, защищённая патентом США [101], содержит приёмопередающую станцию 20 (Боб), кодирующую станцию 10 (Алиса), дуплексную волоконно-оптическую линию 30 (ВОЛ) КРК, а также два

приёмопередатчика, передающий оптический модуль (ПОМ), волоконно-оптический циркулятор (ВОЦ), два приёмных оптических модуля (ПРОМ), направленный волоконно-оптический ответвитель (НВО) X-типа, две ВОЛЗ, два волоконно-оптических фазовых модулятора (ВОФМ), волоконно-оптический поляризационный мультиплексор/демультиплексор (ВОП М/Д), генератор тактовых импульсов (ГТИ), два волновых поляризационных сплиттера, регулируемый волоконно-оптический аттенюатор, два контроллера фазы, два контроллера, банк хранения кодов квантовых состояний фотонов и банк хранения кодов базисов, волновой мультиплексор/демультиплексор, монитор с дисплеем, запоминающее устройство, память (ЛФД₀ и ЛФД₁) (рисунок 2.6). Передатчик и приёмник оптически связаны через ВОЛ.

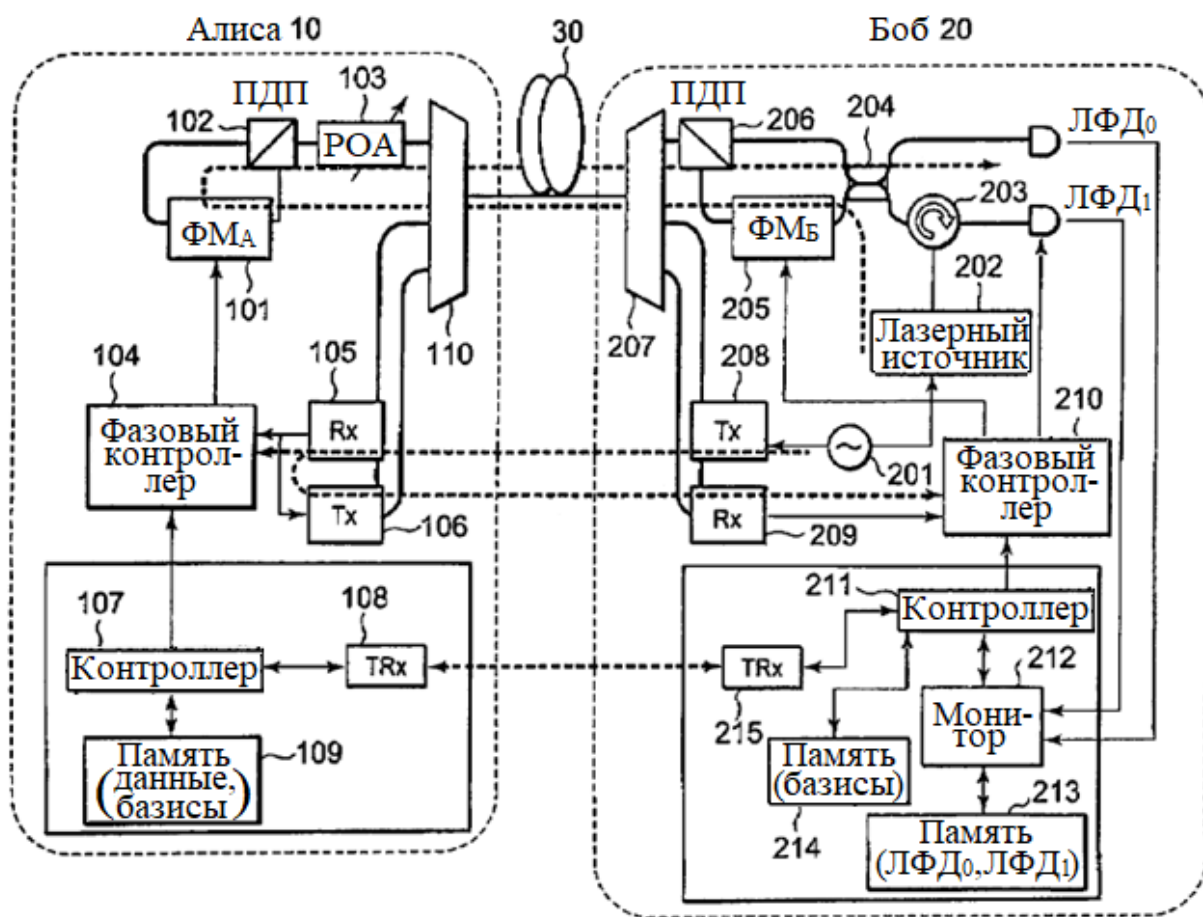


Рисунок 2.6 – Структурная схема системы КРК по патенту US 20070058810

Квантовый блок в передатчике 10 имеет регулируемый оптический аттенюатор (РОА) 103 и петлю с фазовым модулятором (ФМ) 101 и поляризационным делителем пучка (ПДП) 102. Фазовый модулятор 101 выполняет

фазовую модуляцию на последовательности оптических импульсов, проходящих через него, в соответствии с сигналами управления, поступающими от контроллера 104. Фазовая модуляция включает четыре состояния (0 , $\pi/2$, π , $3\pi/2$), соответствующие четырём комбинациям случайного числа, представляющие базис $(+/\times)$, и случайного числа $(0/1)$, представляющего исходные данные для ключа – напряжение, соответствующее любому из состояний модуляции. Сигнал управления фазой подается к фазовому модулятору в момент, когда оптический импульс проходит через фазовый модулятор 101, и, таким образом, оптический импульс становится фазомодулированным. Контроллер фазы 104 применяет сигнал управления фазой к фазовому модулятору 101 в соответствии с тактом синхронизации, полученным от оптического приёмника 105. Выбор момента подачи и уровень напряжения задаются контроллером 107.

ПДП выполняет функцию, подобную зеркалу Фарадея. Входной оптический сигнал в ПДП 102 со стороны приёмника выводится с его поляризационным состоянием, повернутом на 90° [102]. Оптический сигнал, вводимый в квантовый блок от приёмника 20, пропускается через регулируемый оптический аттенюатор 103, поворачивается в ПДП, снова проходит через РОА 103 и затем отсылается назад к приёмнику. РОА 103 устанавливает малое ослабление в режиме синхронизации квантовых блоков и устанавливает большое ослабление при генерации ключа.

Кроме того, у передатчика 10 есть два генератора случайных чисел (не показаны). Контроллер 107 управляет генераторами случайных чисел, первый генератор случайных чисел формирует исходные данные $(0/1)$ для криптографического ключа, другой – генерирует информацию о базисе $(+/\times)$ и последовательно сохраняет генерируемые данные и информацию в памяти 109. Битовые числа каждого из сохранённых случайных чисел управляются при использовании адреса в памяти 109.

Когда процесс генерации ключа запущен, контроллер 107 позволяет РОА 103 увеличить ослабление. Тогда контроллер 107 последовательно считывает наборы исходных данных и информацию о базисах из памяти 109 один за другим и выводит

их на фазовый контроллер 104. Фазовый контроллер выдает сигнал управления фазой, соответствующий каждому набору исходных данных и информации о базисах к фазовому модулятору 101 в соответствии с тактом синхронизации. Модуляция в одном из четырех состояний (0 , $\pi/2$, π , $3\pi/2$) выполняется на каждом из оптических импульсов, проходящих через фазовый модулятор 101.

Для получения сигнала синхронизации, подаваемого на контроллер фазы 104, используется опорный тактовый сигнал, полученный от приёмника через ВОЛ. Опорный тактовый сигнал преобразуется в электрический сигнал оптическим приёмником 105 и подаётся на фазовый контроллер 104. Одновременно опорный тактовый сигнал подаётся на оптический передатчик 106 и на приёмник 20 в качестве опорного тактового сигнала. Контроллер 107 обменивается управляющими сигналами и данными, необходимыми для формирования ключа, синхронизации, коррекции, с контроллером 211 в приёмнике 20 через оптический приёмопередатчик 108.

В данном режиме используется передача с волновым мультиплексированием. Различные длины волн используются для связи между квантовыми блоками, обмена опорными тактовыми сигналами и данными с контроллером 107. Передатчик 10 снабжен волновым демультиплексором 110, который демультиплексирует длины волн приходящих оптических сигналов от ВОЛ и выводит оптические сигналы на РОА 103, оптический приёмник и оптический приёмопередатчик. И наоборот, волновой мультиплексор 110 мультиплексирует длины волн соответствующих оптических сигналов, поступающих от РОА 103, оптического приёмника и приёмопередатчика, и отсылает оптические сигналы в ВОЛ. Таким образом, квантовый и классические каналы объединены в ВОЛ.

Квантовый блок в приёмнике имеет оптический циркулятор 203, оптический ответвитель 204, фазовый модулятор 205, ПДП 206, и лавинные фотодиоды ЛФД₀ и ЛФД₁. Длинный и короткий пути находятся параллельно между оптическим ответвителем 204 и ПДП 206. Фазовый модулятор 205 размещён в длинном пути. Временем приведения в действие и состоянием фазовой модуляции (базиса) управляют с помощью сигнала управления от фазового контроллера 210. Лавинные

фотодиоды ЛФД₀ и ЛФД₁ управляются в стробируемом режиме Гейгера сигналом от фазового модулятора 210 [103].

Приёмник снабжен опорным ГТИ 201. Лазерный источник приводится в действие в соответствии с тактовыми импульсами, генерируемыми ГТИ. Опорный тактовый сигнал передаётся отправителю оптическим передатчиком 208. В отправителе 10 опорный тактовый сигнал используется для определения времени синхронизации и отправляется обратно на приёмник. Опорный тактовый сигнал, возвращённый от отправителя, принимается оптическим приёмником 209 и подаётся на фазовый контроллер 210 в качестве сигнала синхронизации для получателя. Фазовый контроллер 210 управляет временем подачи напряжения на фазовый модулятор 205, а также состоянием фазовой модуляции так, чтобы выбор времени синхронизировать с помощью опорного тактового сигнала. Кроме того, фазовый контроллер 210 управляет временем применения обратного напряжения смещения к фотодетекторам ЛФД₀ и ЛФД₁ для регистрации фотонов.

Приёмник 20 имеет генератор случайных чисел. Контроллер 211 заставляет генератор случайных чисел формировать информацию о базисах (+/×) и последовательно хранит её в памяти 214. Когда начинается процесс формирования ключа, контроллер 211 последовательно считывает информацию о базисах из памяти 214 и выводит её на фазовый контроллер 210. Для памяти 214 используется запоминающее устройство, которое обеспечивает быстрый доступ. Фазовый контроллер 210 подаёт сигналы управления фазой и напряжением, соответствующим выходному базису, к фазовому модулятору 205 в соответствии с опорным тактовым сигналом. Таким образом, модуляция, соответствующая выходному базису, может быть выполнена на оптическом импульсе, посланном от отправителя в момент, когда оптический импульс проходит через фазовый модулятор 205.

Сигналы с фотодетекторов ЛФД₀ и ЛФД₁ последовательно записываются в память 213 как сырой ключ. Битовые числа в данных сырого ключа в памяти 213 и битовые числа, представляющие информацию о базисах в памяти 214 управляются при использовании адреса в соответствующих запоминающих устройствах.

Впоследствии, биты для сырого ключа, записанные в памяти 213, и информация о базисах в памяти 214 сообщаются контроллеру 107 в отправителе 10. Выполняется согласование базисов, чтобы отбросить случайные биты с несовпадающими базисами. В этом случае, как и для тех битов, соответствующих совпавшим базисам, также определяется, совпадают ли данные обнаружения в памяти 213 с исходными данными в памяти 109 и определяется уровень ошибок QBER (Quantum Bit Error Rate). Монитор 212 постоянно отслеживает изменения в уровне ошибок QBER при хранении уровня ошибок QBER в памяти 213. В зависимости от уровня QBER, контроллер 211 выполняет коррекцию фазовых искажений.

В представленном режиме используется волновое мультиплексирование, где различные длины волн используются для квантовой связи, обмена тактовым сигналом эталонной частоты и обмена данными о согласовании базисов с помощью контроллера 211. Получатель 20 снабжен волновым мультиплексором/демультиплексором 207, который демультиплексирует длины волн приходящих оптических сигналов из ВОЛ и выводит оптические сигналы к ПДП 206, оптическому приёмнику 209 и оптическому приёмопередатчику 215. Волновой мультиплексор 207 мультиплексирует длины волн соответствующих оптических сигналов, выходящих от ПДП 206, оптического передатчика 208 и оптического приёмопередатчика 215 и отсылает оптические сигналы в ВОЛ.

Рассмотренные системы КРК и способы синхронизации обладают рядом недостатков. Во-первых, квантовые сигналы и синхросигналы распространяются по отдельным средам (квантовый канал и канал синхронизации соответственно). Во-вторых, отсутствует описание синхросигналов, что означает использование линейного режима синхронизации и, следовательно, мощных синхроимпульсов. Отправка мощных синхроимпульсов по каналу синхронизации значительно упрощает НСД к каналу синхронизации, съём части излучения, внесение помех. Также необходимо отметить отсутствие упоминания о протяжённости каналов, связывающих станции, что говорит о незначительных дальностях передачи.

Таким образом, разработка технического решения подсистемы синхронизации станций системы КРК при обеспечении энергетической скрытности и достаточно протяжённой линии является актуальной проблемой.

Одно из направлений обеспечения скрытности процесса синхронизации станций системы КРК заключается в использовании однофотонного режима передачи. Необходимо отметить, не существует технического решения синхронизации станций при использовании однофотонного режима передачи, защищённого патентом, что также указывает на актуальность исследований.

В [104] представлено техническое решение подсистемы синхронизации станций системы КРК с однофотонным уровнем передачи синхрои импульсов. По сравнению с подсистемами синхронизации с использованием многофотонного режима, недостаток данного решения состоит в ограниченной протяжённости ВОЛС и значительных временных затратах при поиске синхрои импульса [24], который предполагает анализ временного кадра, равного по длительности периоду следования синхрои импульсов, на предмет наличия фотонов и/или ИТТ.

Проведённый анализ позволяет сформулировать цель диссертационных исследований, которая заключается в увеличении протяжённости ВОЛС в системе КРК на однофотонных ЛФД при сохранении энергетической скрытности синхронизации.

Резюме. В ходе анализа технических решений и принципов функционирования подсистем синхронизации выявлены их конструктивные и функциональные недостатки. Обоснована целесообразность разработки алгоритма подсистемы синхронизации станций системы КРК с увеличением протяжённости ВОЛС. Для сохранения энергетической скрытности синхронизации и, следовательно, повышения безопасности процесса синхронизации принято использование однофотонного режима передачи.

2.2 Синтез двухэтапного временного алгоритма синхронизации системы квантового распределения ключа

Проанализируем работу системы КРК с автоматической компенсацией поляризационных искажений [32], состоящую из приёмопередающей и

кодирующей станций. Биты ключа кодируются изменением фазовых состояний фотонов в фотонном импульсе. От приёмопередающей станции к кодирующей станции распространяются оптические импульсы со средним числом фотонов значительно превышающем единицу ($\mu \gg 1$). В обратном направлении – от кодирующей станции к приёмопередающей станции уже действуют фотонные импульсы со средним числом фотонов не более 1 ($\mu < 1$).

Исследования проводятся при ряде предположений.

Предположение 1. Априорная информация о расстоянии между станциями отсутствует. Известно лишь предполагаемое максимальное расстояние L_{FOL} .

Предположение 2. Фотон с равной вероятностью может появиться в любой момент внутри фотонного импульса. Последнее предполагает прямоугольную форму исходного лазерного импульса (появления фотона в фиксированном временном интервале). Данное предположение следует из того факта, что длительность оптического импульса лазера в системе КРК (300 пс для системы компании ID Quantique) значительно превышает время анализа любого участка ВОЛС.

Предположение 3. Используется идеальный лазер, генерирующий фотоны с фиксированной длиной волны. Это исключает необходимость учёта хроматической дисперсии в ВОЛС и, следовательно, размытия фотонного импульса (разброса момента приёма фотона).

Предположение 4. Статистические свойства потока фотонов, ИТТ и послеимпульсов описываются законом Пуассона $Pr\{k|\mu\} = (\mu^k/k!) \cdot \exp(-\mu)$. Здесь вероятность генерации равно k событий определяется средним числом событий за время наблюдения (длительность временного кадра, фотонного импульса или импульса стробирования) μ .

Однофотонный алгоритм синхронизации предусматривает разбиение временного кадра на интервалы. Каждый интервал соответствует определённому участку ВОЛС. Алгоритм последовательно опрашивает участки с убывающей длиной. Последнее позволяет значительно уменьшить влияние ИТТ ОЛФД за

время анализа участка. Благодаря этому увеличивается отношение сигнал/шум [105].

Пусть подсистема синхронизации с последовательным опросом участков ВОЛС выполнена на оптическом волокне с погонным затуханием α_{OF} и показателем преломления оптического излучения в сердцевине n_{OF} . Зная скорость распространения излучения в вакууме $c_{opt} = 300\,000$ км/с, находим скорость распространения излучения в сердцевине оптического волокна

$$v_{OF} = c_{opt}/n_{OF}. \quad (2.1)$$

Частота генерации ИТТ в фотодетекторе равна ξ_{DCR} . Передатчик генерирует оптические импульсы длительностью τ_s . Нестабильность периода следования синхроимпульсов исключается ($\Delta T_s = 0$).

Среднее число фотонов за длительность оптического импульса на выходе из кодирующей станции – $\overline{n_{s0}}$.

Введём обозначения $P_{err.test.0}$ и $P_{err.0}$ соответственно для допустимых вероятностей ошибки тестирования и ошибки синхронизации.

Пусть ВОЛС с длиной L_{FOL} разбита на N_{FOL} участков с убывающей длиной $l_j, j = \overline{1, N_{FOL}}$ (рисунок 2.7). Причём, всегда выполняются условия

$$L_{FOL} = \sum_{j=1}^{N_{FOL}} l_j \quad \text{и} \quad l_{j-1} > l_j, \quad j = \overline{2, N_{FOL}}. \quad (2.2)$$

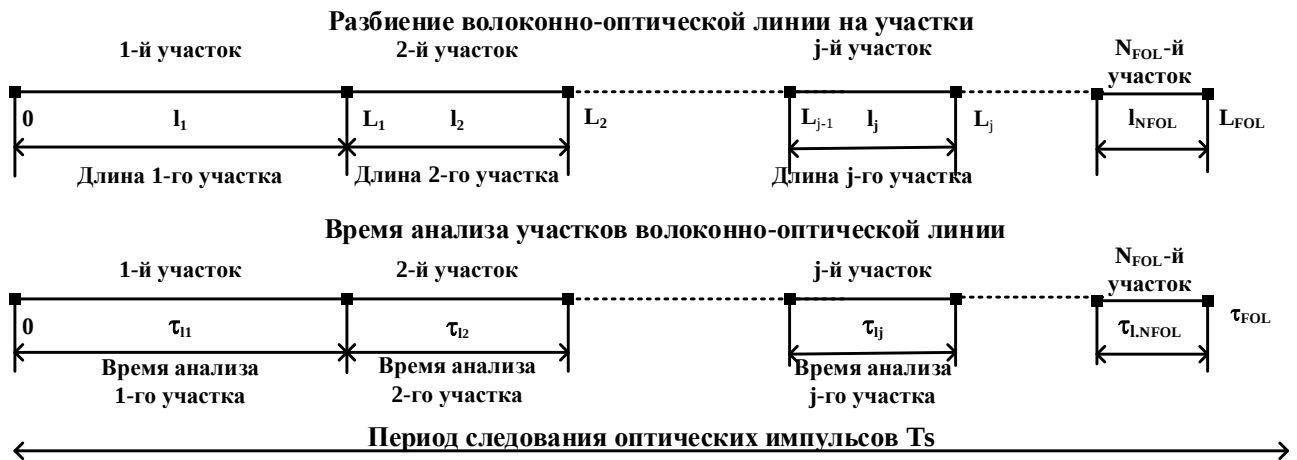


Рисунок 2.7 – Разбиение волоконно-оптической линии на участки
Верхняя граница j -го участка определяется формулой

$$l_j = \begin{cases} L_1, & \text{при } j = 1; \\ L_j - L_{j-1}, & \text{при } j = \overline{2, N_{FOL}}. \end{cases} \quad (2.3)$$

Для расчёта времени анализа j -го участка ВОЛС справедлива формула

$$\tau_{l_j} = 2 \cdot l_j / v_{OF}. \quad (2.4)$$

При ориентации на предельно-возможное разнесение L_{FOL} приёмопередающей и кодирующей станций автокомпенсационной системы КРК период следования оптических синхроимпульсов должен удовлетворять условию

$$T_s \geq T_{s.min} = 2 \cdot L_{FOL} / v_{OF}. \quad (2.5)$$

Множитель 2 в формулах (2.4) и (2.5) учитывает, что в автокомпенсационной системе КРК фотон дважды проходит ВОЛС: приёмопередающая станция $\rightarrow$ ВОЛС $\rightarrow$ кодирующая станция $\rightarrow$ ВОЛС $\rightarrow$ приёмопередающая станция.

Идея последовательного анализа участков ВОЛС с убывающей длиной связана с уменьшением среднего числа ИТТ за время анализа каждого последующего участка ВОЛС (при одновременном снижении энергии в фотонном импульсе). Причём обеспечивается такая пропорция между средним числом ИТТ за время анализа участка и средним числом фотонов в фотонном импульсе на верхней границе участка, которая гарантирует высокую (не ниже требуемой) вероятность синхронизации.

В предлагаемом алгоритме аппаратура на этапе поиска анализирует 1-й временной интервал в первом кадре, соответствующий времени анализа первого участка волоконно-оптической линии связи, на наличие фотона или ИТТ. При отрицательном результате поиска в первом участке первого кадра, аппаратура переходит к анализу последующих временных кадров. При положительном результате поиска аппаратура начинает этап тестирования, причем повторный опрос фотодетектора производится в течение длительности импульса стробирования. Поиск фотона в 1-м участке ВОЛС показан на рисунке 2.8.

На этапе поиска каждому участку ВОЛС соответствует определенное число кадров (для 1-го участка $a_{1.N11} \geq i_{l_1} \geq a_{1.1} = 1$). Блок тестирования в каждом временном кадре внутри одного участка ВОЛС будет идентичен, количество тестов равно b_{N2} . При переходе к исследованию следующих участков в блоке

тестирования будет меняться только максимальное допустимое количество тестов, которое зависит от номера участка ВОЛС.

Вероятность повторного обнаружения синхроимпульса p_2 определяется вероятностью регистрации суммарного количества сигнальных и шумовых импульсов, отличного от 0.

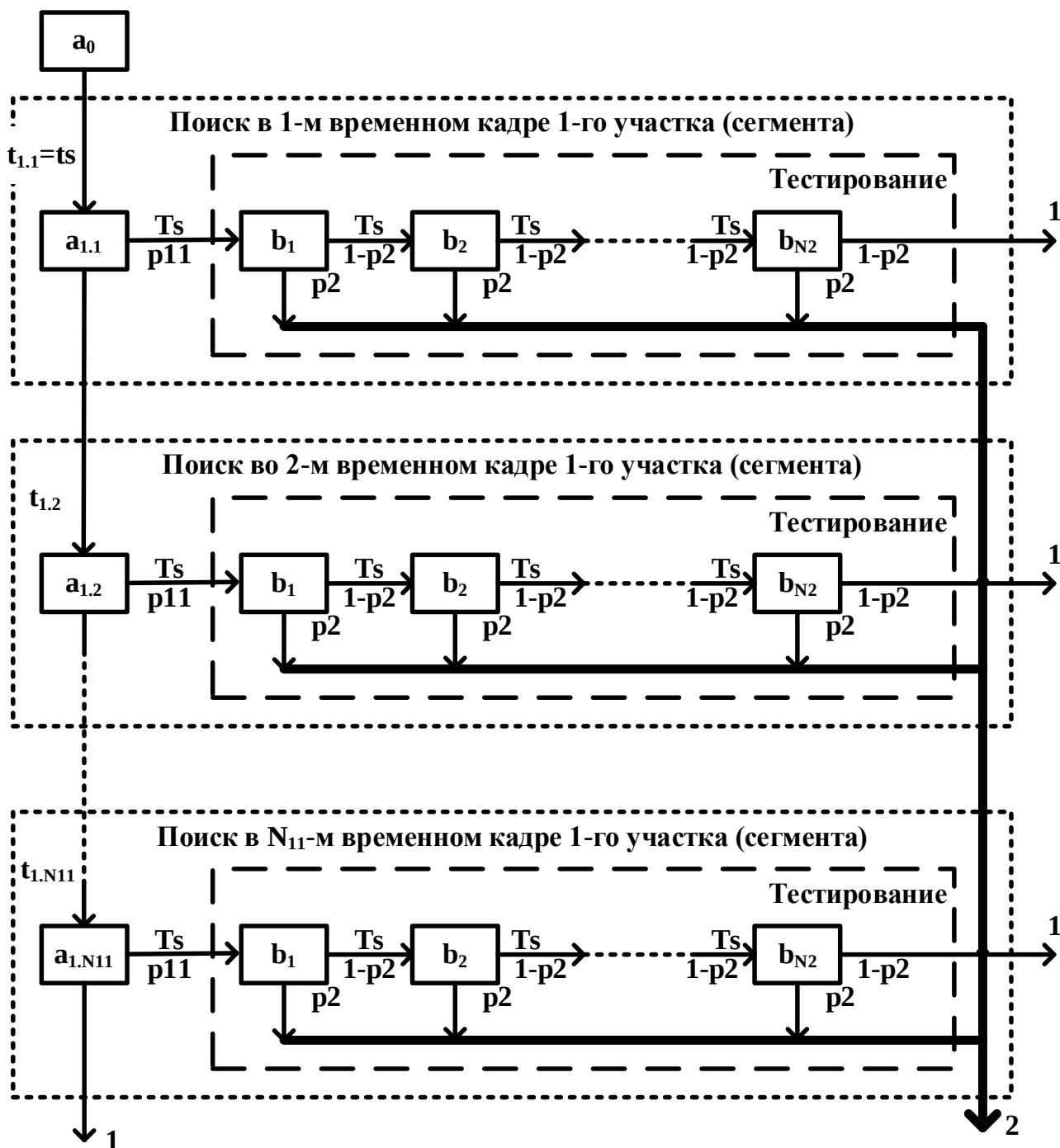


Рисунок 2.8 – Алгоритм поиска однофотонного излучения в 1-м участке ВОЛС

В случае отрицательного результата тестирования (выход 1) можно говорить, что произошло ложное срабатывание. После ложного срабатывания аппаратура

вновь возвращается в режим поиска. Причём теперь проверяется уже второй участок ВОЛС. Аналогичный переход к анализу следующего участка осуществляется также при отрицательном результате поиска. Выход 2 означает успешный результат тестирования.

Резюме. Предложен алгоритм синхронизации приёмопередающей и кодирующей станций с фазовым кодированием состояний фотонов в автокомпенсационной системе квантового распределения ключа. Отличительной особенностью алгоритма является разбиение волоконно-оптической линии на участки с убывающей длиной, что позволяет значительно уменьшить влияние ИТТ ОЛФД за время анализа участка.

2.3 Обоснование типовой структуры программно-аппаратного комплекса для передачи конфиденциальной информации

Типовая структурная схема комплекса для передачи конфиденциальной информации с автокомпенсационной системой КРК представлена на рисунке 2.9.

В приведённой схеме источник данных формирует цифровые сигналы, соответствующие определённому виду информации телекоммуникации (см. ГОСТ 22670-77). В электронном шифраторе, используя секретный ключ, осуществляется криптографическая обработка (шифрование) параметров цифровых сигналов для защиты информации от НСД. В комплексе MagiQ QPN-5505 данные на канальном уровне шифруются с помощью симметричного алгоритма блочного шифрования AES-256.

Для дальнейшей передачи зашифрованных данных используется волоконно-оптический канал, представляющий совокупность технических средств (оптического передатчика и оптического приёмника) и ВОЛС. Канал по ОВ формирует маршрут передачи данных между пользователями.

В реализуемой симметричной криптосистеме пользователи используют общий секретный ключ, который периодически и одновременно обновляется. В комплексе эту функцию выполняет система КРК, которая состоит из кодирующей и приёмопередающей станций. Станции имеют управляющие входы и выходы для

синхронизации своей работы, контроля параметров системы КРК и управления волоконно-оптической системой передачи данных.

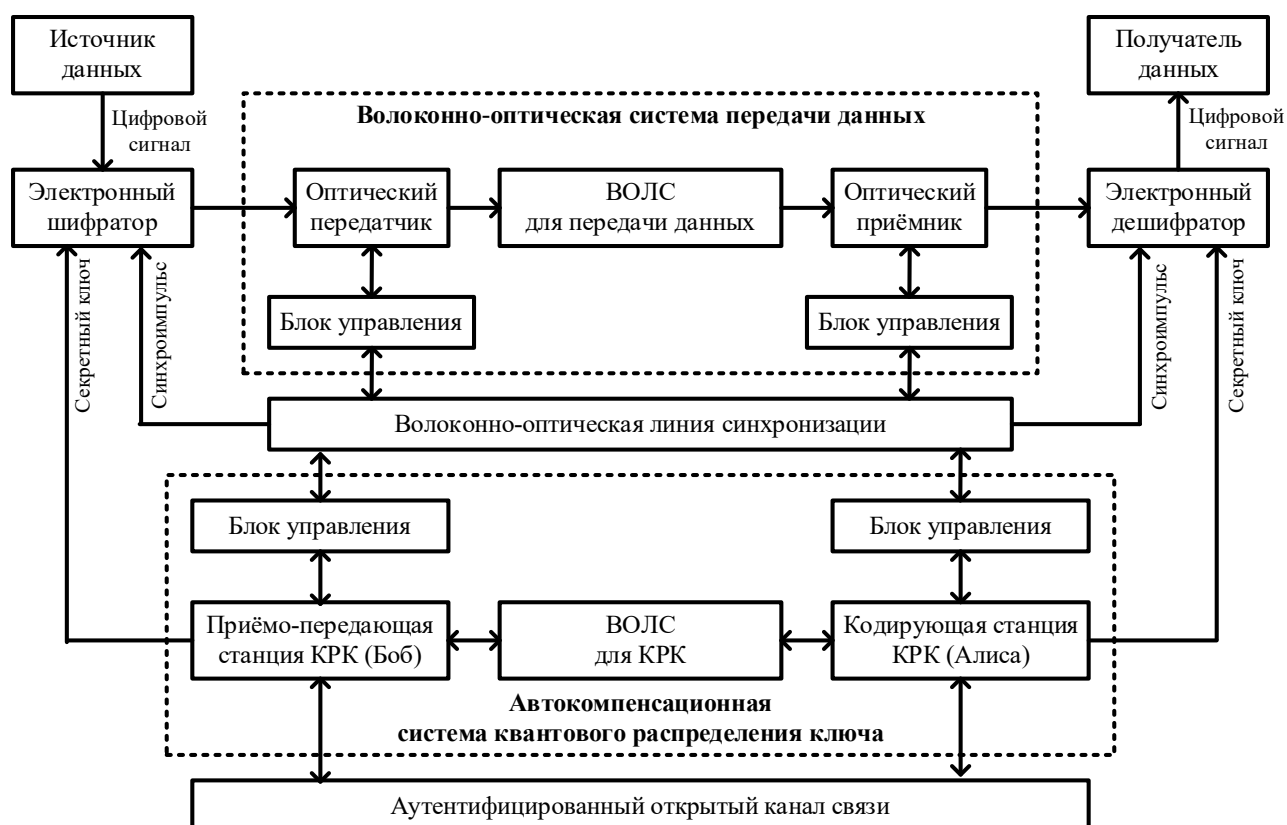


Рисунок 2.9 – Типовая структура программно-аппаратного комплекса для передачи конфиденциальной информации

Типовая система КРК включает приёмопередающую и кодирующую станции, соединённые ВОЛС. Формирование секретных ключей происходит передачей одиночных фотонов через ВОЛС. Общий секретный ключ распределяется его между законными пользователями (источником и получателем данных на рисунке 2.9). С помощью этого ключа производится как шифрование данных источника, так и дешифрование данных пользователями.

Программное обеспечение блоков управления формирует управляющие команды. Посредством 4-х блоков управления и ВОЛС обеспечивается синхронизация разнесённых в пространстве оптических станций волоконно-оптической системы передачи данных, электронных шифратора и дешифратора, а также приёмопередающей и кодирующей станций системы КРК. Отмечается, что точность синхронизации в пределах десятков пикосекунд сильно влияет на общие характеристики программно-аппаратного комплекса для передачи конфиденциальной информации.

Аутентифицированный открытый канал связи предназначен для проверки совпадения базиса кодирования квантового состояния фотона с базисом измерения состояния фотона. Этот канал может не быть конфиденциальным, только подлинным. Следовательно, злоумышленник может иметь доступ к открытому каналу связи, но не может изменять передаваемую через канал информацию.

Отметим, что в описанном комплексе для передачи информации можно использовать только одну ВОЛС для организации передачи данных, КРК, синхронизации и аутентифицированного открытого канала связи. Например, это возможно, используя волновое или временное мультиплексирование/демультиплексирование. Следовательно, квантовое распределение ключа может осуществляться как по индивидуальному оптическому волокну, так и посредством интегрирования в информационную ВОЛС. Дальность связи по одномодовому ОВ близка к 100 км.

Резюме. Обоснована типовая структура программно-аппаратного комплекса для передачи конфиденциальной информации посредством КРК. Структура комплекса включает четыре канала: канал передачи данных, канал синхронизации, канал КРК и аутентифицированный открытый канал. Периодическое обновление секретного ключа одновременно у двух пользователей выполняется системой КРК с кодирующей и приёмопередающей станциями. Станции имеют управляющие входы и выходы для синхронизации своей работы, контроля параметров системы КРК и управления волоконно-оптической системой передачи данных.

2.4 Анализ структуры станций системы КРК с фазовым кодированием состояний фотонов по протоколу BB84

В типовой структуре системы, использующей протокол BB84 с кодированием состояния фотона по фазе, приёмопередающая станция посредством оптического фазового модулятора (ОФМ_Б) вносит один из четырёх фазовых сдвигов (0 , $\pi/2$, π , $3\pi/2$), генерируя фотон в одном из четырёх квантовых состояний. Биту «0» соответствуют фазовые сдвиги 0 и $\pi/2$, а биту «1» – сдвиги π и $3\pi/2$. В свою очередь, кодирующая станция посредством фазового модулятора ОФМ_А производит случайный выбор базиса измерения, сдвигая фазу на 0 или $\pi/2$. Фотону,

пришедшему на первый однофотонный приёмник ОФП₁, присваивается бит «0», а фотону, принятому вторым приёмником ОФП₂, – бит «1».

Когда разности фаз равны 0 или π , то в приёмопередающей и кодирующей станциях используются совместимые базисы. В таких случаях кодирующая станция может определить, в какой из однофотонных приёмников ОФП₁ или ОФП₂ приёмопередающей станции попал фотон, и, следовательно, она может определить значение бита. Со своей стороны, приёмопередающая станция может определить, какая фаза выбрана кодирующей станцией при передаче фотона. В случае, когда разность фаз принимает значения $\pi/2$ или $3\pi/2$, стороны используют несовместимые базисы, и фотон случайным образом регистрируется в одном из ОФП приёмопередающей станции.

Возможные комбинации фазовых состояний фотона при реализации протокола BB84 с четырьмя состояниями даны в таблице 2.1.

Проанализируем типовую структуру приёмопередающей станции автокомпенсационной системы (рисунок 2.10), где совмещены функции передачи и приёма. Станция предназначена для генерации оптических импульсов, формирования фотонных импульсов, приёма и обработки закодированных квантовых состояний фотонов.

Таблица 2.1 – Возможные комбинации квантовых состояний фотонов при фазовом кодировании по протоколу BB84

Значение исходного бита	Фазовый сдвиг ФБ приёмопередающей станции	Фазовый сдвиг ФА кодирующей станции	Разность фаз ФБ–ФА	Значение регистрируемого бита
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	неопределенно
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	неопределенно
0	$\pi/2$	0	$\pi/2$	неопределенно
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	неопределенно
1	$3\pi/2$	$\pi/2$	π	1

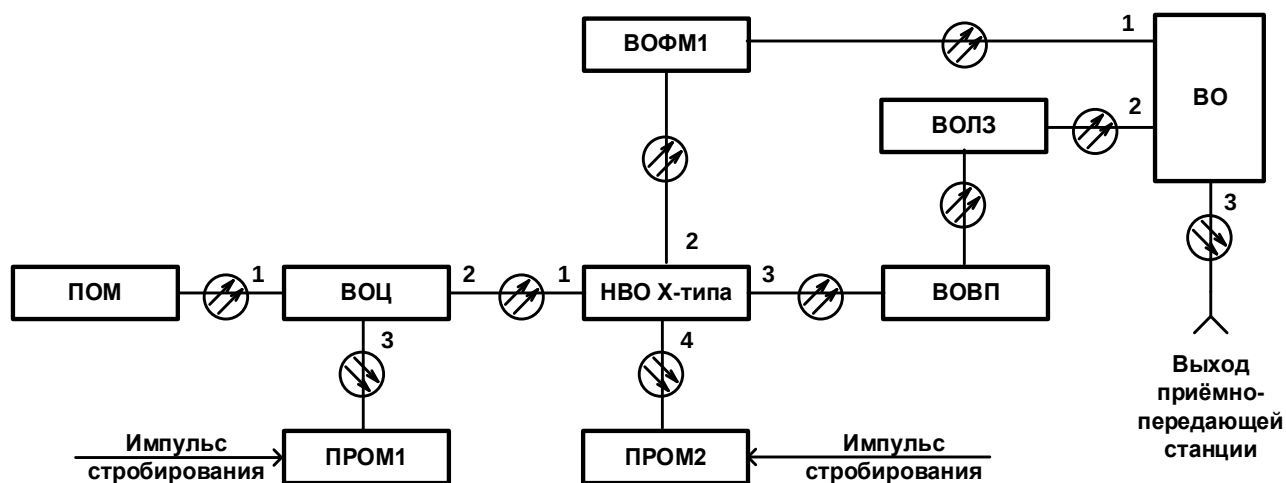


Рисунок 2.10 – Структура оптической части приёмопередающей станции

В состав приёмопередающей станции входит ПОМ, циркулятор ВОЦ с циркуляцией по часовой стрелке, интерферометр Маха-Цендера, два ПРОМ на ОЛФД, способных регистрировать одиночные фотоны.

Передающий оптический модуль строится на основе импульсного когерентного лазера. Выходное излучения лазера должно иметь строго определённую поляризацию (далее предполагается вертикальная поляризация).

Лазерный импульс с длиной волны 1550 нм излучается передающим оптическим модулем и посредством волоконно-оптического циркулятора направляется на вход интерферометра, являющийся входом НВО X-типа.

Интерферометр станции содержит направленный волоконный ответвитель (НВО) X-типа, первый волоконно-оптический фазовый модулятор (ВОФМ1), волоконно-оптический вращатель поляризации (ВОВП) на $\pi/2$, ВОЛЗ и волоконный ответвитель (ВО). Оптическое волокно, сохраняющее поляризацию оптического излучения, соединяет перечисленные функциональные блоки.

Лазерный импульс с верхнего порта НВО X-типа, имеющий вертикальную поляризацию, через ВОФМ1 попадает на 1-й порт волоконного ответвителя (см. рисунок 2.10). Для реализации протокола BB84 на приёмопередающей станции фотон в импульсе сдвигается по фазе на одно из случайно выбираемых значений из ряда 0, $\pi/2$, π , $3\pi/2$.

Поляризация фотонного импульса с 3-го порта НВО X-типа по пути к 2-му порту волоконного ответвителя посредством волоконно-оптического вращателя

поляризации изменяется на угол $\pi/2$. Следовательно, на 2-м порте волоконного ответвителя оптическое излучение имеет уже горизонтальную поляризацию.

Волоконный ответвитель является пассивным элементом, выход которого является выходом приёмопередающей станции.

В результате распространения лазерных импульсов по двум разным оптическим плечам интерферометра и включения ВОЛЗ в его нижнее плечо формируется опорный (первый по времени) импульс с вертикальной поляризацией и дублирующий (второй по времени) импульс с горизонтальной поляризацией. Причём дублирующий импульс запаздывает относительно опорного импульса на 50 нс.

В состав кодирующей станции входят регулируемый волоконно-оптический аттенюатор, волоконно-оптический фазовый модулятор (ВОФМ2), зеркало Фарадея (рисунок 2.11). Все блоки соединены между собой стандартным оптическим волокном.

Зеркало Фарадея представляет вращатель с фиксированным углом поворота поляризации на $\pi/2$. Поэтому отражённые фотонные опорный и дублирующий импульсы уже не только ортогонально поляризованы относительно друг друга, но и ортогонально поляризованы относительно первичных импульсов на входе зеркала Фарадея.

На кодирующей станции посредством второго волоконно-оптического фазового модулятора фотон в дублирующем импульсе сдвигается по фазе на одно из двух случайно выбираемых неортогональных значений из ряда 0 и $\pi/2$.

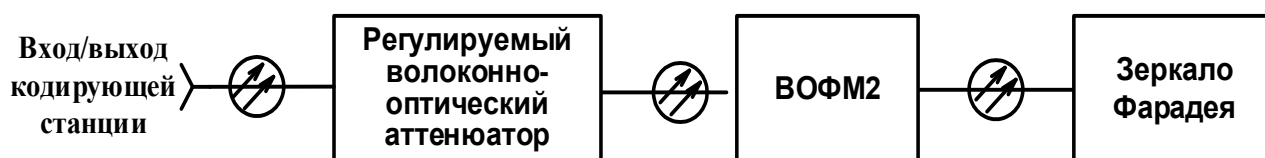


Рисунок 2.11 – Структурная схема кодирующей станции системы

За счёт двойного прохождения через регулируемый аттенюатор формируются фотонные импульсы, где среднее число фотонов за их длительность не превышает 0,1...0,5. Это гарантирует безопасность распределения ключа.

Опорный и дублирующий фотонные импульсы на обратном пути от кодирующей станции проходят ВОЛС и волоконно-оптический поляризационный ответвитель в приёмопередающей станции. Поскольку эти импульсы ортогонально поляризованы относительно первичных сигналов, они попадают в плечо интерферометра, по которому не распространялись при прямом прохождении. Здесь волоконный ответвитель выступает в роли поляризационного делителя.

Опорный и дублирующий фотонные импульсы попадают на НВО Х-типа одновременно и интерферируют между собой. Результат интерференции регистрируется первым или вторым ПРОМ.

Так как оба импульса проходят один и тот же оптический путь, то в системе QPN-5505 автоматически компенсируются поляризационные искажения.

Синхронизация станций обеспечивается с помощью дополнительной волоконно-оптической линии и дополнительных модулей. В приёмопередающей станции квантовым лазером генерируются оптические тактовые синхроимпульсы, инициализируются временные характеристики системы. Тактовые синхроимпульсы с периодом следования примерно 1,645 мкс распределяются по функциональным узлам, обеспечивая подачу электронного импульса:

- на первый волоконно-оптический фазовый модулятор ВОФМ1 приёмопередающей станции во время прохождения через него лазерного импульса;
- на второй фазовый модулятор ВОФМ2 кодирующей станции во время прохождения через него дублирующего фотонного импульса;
- на однофотонные ЛФД во время ожидаемого приёма фотонного импульса после интерференции для перевода фотодетекторов в режим регистрации фотона.

Временные интервалы каждого из приведённых действий определяются длинами волоконно-оптических линий (КРК и синхронизации) и электрических кабелей, а также временными задержками в функциональных узлах.

В таблице 2.2 приведены стандартные значения временных задержек основных функциональных узлов системы с комментариями.

Время распространения фотона между станциями равно периоду следования тактовых синхроимпульсов $T_s=1,645$ мкс. Данный период следования обеспечивает

прохождение фотоном станций и ВОЛС (протяженность которой не превышает 160 м) и отсутствие наложения генерируемых фотонов друг на друга. Один период соответствует одному биту. Однако при увеличении протяженности ВОЛС свыше 160 м обнаружение фотона будет происходить уже в новом периоде следования, в котором сгенерирован новый фотон. Таким образом, при генерации и обнаружении фотона в разных битах (периодах) необходима синхронизация последних. Для этого должна быть введена соответствующая электронная задержка – регулировка битового сдвига (Bit Skew) в приёмопередающей и кодирующей станциях.

Таблица 2.2 – Значения временных задержек компонентов системы

Функциональный узел	Значение временной задержки	Комментарии
Лазер	10 ... 1 500 нс	Генерируется импульс с минимальной длительностью для стабильной работы системы (обычно 500...1000 пс).
ОЛФД1	Время распространения фотона в ВОЛС рассчитывается исходя из 5 мкс на километр ОВ.	ОЛФД переводится в режим регистрации фотона (точность подачи импульса стробирования обычно равна 100 пс).
ОЛФД2	Время задержки в ОЛФД2 устанавливается с учётом задержки в ОЛФД1.	
ВОФМ1	Задержка предшествует задержке ОЛФД1 (менее 200 нс). Это значение фиксируется внутренними параметрами станции и не изменяется.	Рекомендуемая длительность электрического импульса на модуляторе равна 45 нс. Если время задержки в модуляторе установлено правильно, то сдвиг фазы не зависит от состояния поляризации излучения. Плавный изгиб или скручивание ОВ не должно существенно влиять на время распространения сигнала между ОЛФД.
ВОФМ2	Временная задержка равна времени распространения излучения от лазера до кодирующей станции.	

Настройка битового сдвига не влияет на работу системы в режиме калибровки. Однако даже при нормальном функционировании системы в режиме калибровки, если регистры битового сдвига установлены неправильно, то в режиме КРК частота ошибок может приближаться к 50%.

Увеличение битового сдвига на одну позицию изменяет внутреннюю электронную задержку примерно на период следования $T_s=1,645$ мкс.

Резюме. Проведён анализ типовой структуры станции автокомпенсационной системы. Отличительной особенностью системы является обеспечение безопасности КРК, достигаемое за счёт формирования фотонных импульсов со среднем числом фотонов $0,1...0,5$ после двойного прохождения через регулируемый волоконно-оптический аттенуатор в кодирующей станции. Проанализированы возможные комбинации фазовых состояний протокола для станций. Значение регистрируемого бита считается достоверно известным при разности фаз приёмопередающей и кодирующей станций 0 или π .

2.5 Техническое решение двухэтапного алгоритма однофотонной синхронизации

Рассмотрим структурную схему подсистемы предварительной однофотонной синхронизации для автокомпенсационной системы КРК (рисунок 2.12), реализующую предлагаемый двухэтапный алгоритм синхронизации.

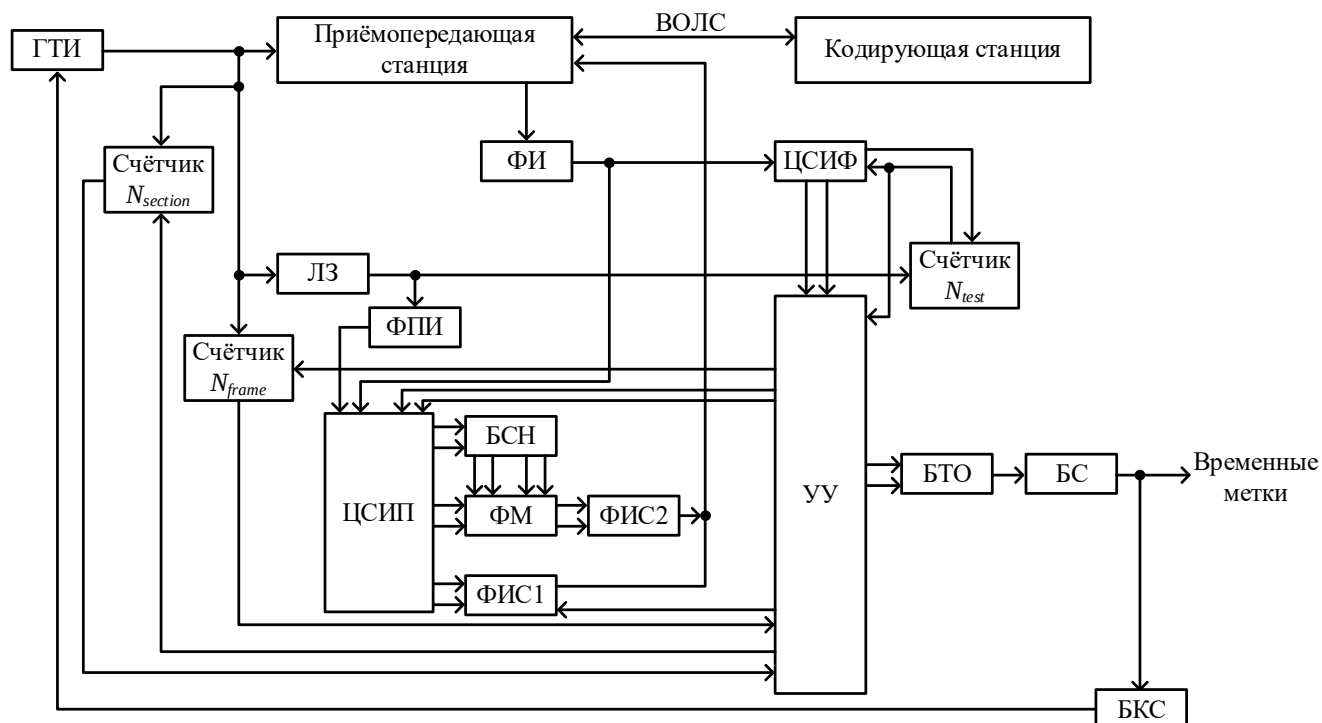


Рисунок 2.12 – Структурная схема подсистемы синхронизации

Запуск процесса синхронизации приёмопередающей и кодирующей станций начинается с генерации импульсов генератором тактовых импульсов (ГТИ) с заданным периодом следования. Тактовые импульсы в количестве N_{frame} и $N_{section}$

поступают на входы приёмопередающей станции, линии задержки и счётчиков. При получении импульса приёмопередающая станция генерирует оптический импульс на заданной длине волны. Оптический импульс поступает на вход кодирующей станции через ВОЛС. После прохождения кодирующей станции оптический импульс возвращается обратно на вход приёмопередающей станции посредством ВОЛС для детектирования. Таким образом, оптический импульс проходит ВОЛС дважды. Причём, зная скорость распространения оптического излучения в ОВ, можно определить временной интервал поступления оптического импульса в детекторный блок приёмопередающей станции. Временной интервал окружён защитными отрезками, в которых гарантировано отсутствие синхроимпульса. Реализация защитного интервала обеспечивается линией задержки (ЛЗ), с которой тактовые импульсы с заданной задержкой поступают на формирователь пачки импульсов (ФПИ) и счетчик N_{test} . Отметим, режим синхронизации протекает в однофотонном режиме.

Формирователь импульсов (ФИ) формируется после детектирования из принятого сигнала видеоимпульс.

Счётчики $N_{section}$ и N_{frame} обеспечивают контроль максимального числа участков ВОЛС и максимального числа кадров для каждого участка на этапе поиска. Работой счётчиков управляет устройство управления (УУ). При переполнении счётчиков формируется сигнал ошибки, поступающий на вход УУ.

Работой счётчика N_{test} управляет цифровой счётчик импульсов фотонов (ЦСИФ). Счётчик N_{test} характеризуется максимальным количеством тестов на этапе тестирования. При его превышении формируется сигнал прерывания, поступающий на УУ. Подсистема синхронизации переводится в режим поиска на интервале $[0; T_s]$, счётчик N_{test} обнуляется.

ЦСИФ передает УУ двоичный код по двухразрядной шине, сформированный на основе сигналов от ФИ. Двоичный код «01» – регистрация фотонного импульса на этапе поиска, переход к этапу тестирования. Код «10» – повторная регистрация фотонного импульса на этапе тестирования, успешное обнаружение синхроимпульса. Счётчик ЦСИФ обнуляется при переполнении счётчика N_{test} .

Цифровой счётчик импульсов пачки (ЦСИП) подсчитывает и нумерует временные метки, в качестве которых используется пачка импульсов с ФПИ. Шаг следования импульсов равен 1 нс. Работой ЦСИП управляет УУ.

При поступлении на ЦСИФ сигнала регистрации фотонного импульса на этапе поиска фиксируется номер ближайшей временной метки, пришедшей от ФПИ. Далее номер временной метки передаётся по двухразрядной шине в блок сдвига номера (БСН) для определения номеров предыдущей и последующей меток. Эти граничные номера меток определяют интервал стробирования на этапе тестирования. Полученные номера меток поступают по шинам на формирователь меток (ФМ). При последующих тестах ФМ сравнивает номера поступающих от ЦСИФ временных меток с определёнными ранее. При достижении ЦСИФ номера нижней или верхней граничной метки ФМ отправляет соответствующий импульс на формирователь импульсов стробирования (ФИС2). ФИС2 формирует строб-импульс по полученным номерам граничных меток. Далее стробирующий импульс направляется на приёмопередающую станцию. ФИС1 формирует строб-импульс длительностью $[0; T_s]$ по первой и последней меткам в пачке импульсов от ФПИ на этапе поиска.

В результате процесса синхронизации УУ формирует следующие двоичные коды: «00» – этап поиска синхросигнала; «01» – этап тестирования; «10» – синхроимпульс обнаружен, синхронизация установлена; «11» – обрыв ВОЛС, отсутствие ФИ, ошибка.

Предложенное техническое решение автокомпенсационной системы КРК обеспечивает повышенную безопасность в связи с использованием однофотонного режима синхронизации. Благодаря разбиению ВОЛС на участки с убывающей длиной возможно увеличение протяжённости ВОЛС при обеспечении заданной вероятности ошибки синхронизации.

Резюме. Предложена и проанализирована структура подсистемы синхронизации станций в системе КРК согласно разработанному двухэтапному алгоритму, учитывающему параметры реального используемого ОЛФД.

2.6 Выводы к главе 2

Проведённый анализ технических решений и принципов функционирования подсистем синхронизации позволил выявить их конструктивные и функциональные недостатки. Обоснована целесообразность разработки алгоритма подсистемы синхронизации системы КРК с увеличением протяжённости ВОЛС. Для сохранения энергетической скрытности синхронизации и, следовательно, повышения безопасности процесса синхронизации принято использование однофотонного режима передачи.

Проанализирована типовая структура программно-аппаратного комплекса для передачи конфиденциальной информации, использующего протокол BB84. В системе два основных канала: канал КРК и канал синхронизации. Последний включается путём мультиплексирования линии для синхронизации станций (1550 нм) и линии для информационных данных (1310 нм).

Предложен алгоритм синхронизации станций автокомпенсационной системы КРК с фазовым кодированием состояний фотонов. Предложена и описана структурная схема подсистемы синхронизации станций в системе КРК согласно разработанному двухэтапному алгоритму, учитывающему параметры используемого ОЛФД. Однофотонный алгоритм синхронизации предусматривает разбиение временного кадра на интервалы. Каждый интервал соответствует определённому участку ВОЛС. Алгоритм последовательно опрашивает участки с убывающей длиной. Последнее позволяет значительно уменьшить влияние ИТТ ОЛФД за время анализа участка. Благодаря этому увеличивается отношение сигнал/шум.

Результаты проведённых исследований отражены в статьях [18, 20, 23, 105] и апробированы на научно-технических конференциях: International Conference on Futuristic Trends in Networks and Computing Technologies, FTNCT 2019, 22-23 ноября 2019, Чандигарх, Индия; V, VII Всероссийские научно-технические конференции молодых ученых, аспирантов, магистрантов и студентов «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности», 01-07 апреля 2019, 5-11 апреля 2021, Таганрог;

I Всероссийская Научно-Практическая Конференция «Digital Era», 26 марта 2021,
г. Грозный.

3. ОЦЕНКА ЭФФЕКТИВНОСТИ ДВУХЭТАПНОГО АЛГОРИТМА СИНХРОНИЗАЦИИ

3.1 Оценка вероятностных характеристик двухэтапного временного алгоритма синхронизации

Пусть подсистема синхронизации с последовательным опросом участков ВОЛС выполнена на ОВ с погонным затуханием α_{OF} и показателем преломления оптического излучения в сердцевине n_{OF} . Зная скорость распространения излучения в вакууме $c_{opt} = 300\,000$ км/с, находим скорость распространения излучения в сердцевине ОВ по формуле (2.1).

Частота генерации ИТТ в фотодетекторе равна ξ_{DCR} . Передатчик генерирует оптические импульсы длительностью τ_s . Нестабильность периода следования синхроимпульсов исключается ($\Delta T_s = 0$).

Среднее число фотонов за длительность оптического импульса на выходе из кодирующей станции – $\overline{n_{s0}}$.

Введём обозначения $P_{err.test.0}$ и $P_{err.0}$ соответственно для допускаемых вероятностей ошибки тестирования и ошибки синхронизации.

Для описанного алгоритма, как показано в [16], вероятность ошибки синхронизации по итогам двух этапов при нахождении кодирующей станции в j -м участке ВОЛС описывается формулой

$$P_{err.j} = 1 - P_{D.j} \cdot (1 - P_{err.test.j}), \quad (3.1)$$

где

$$P_{D.j} = \frac{1 - \exp(-\overline{n_{DCR.j}})}{\overline{n_{DCR.j}}} \cdot \frac{1 - P_{DCR.j}^{N_j}}{1 - P_{DCR.j}} \cdot P_{Ds.j} \quad (3.2)$$

– вероятность обнаружения фотонного импульса на этапе поиска за N_j временных кадров в j -м участке с учётом равномерного распределения момента появления оптического импульса на интервале наблюдения;

$$P_{err.test.j} = \exp(-N_{test.j} \cdot \overline{n_{strob.j}}) \quad (3.3)$$

– вероятность ошибки тестирования (отсутствие регистрации фотонов и ИТТ за время всех допустимых $N_{test,j}$ тестов при анализе j -го участка ВОЛС).

В формулах (3.2) и (3.3) используются следующие обозначения:

– среднее число ИТТ за время анализа j -го участка ВОЛС

$$\overline{n_{DCR,j}} = \xi_{DCR} \cdot \tau_{l,j} ; \quad (3.4)$$

– вероятность отсутствия регистрации фотонов и ИТТ за время анализа j -го участка ВОЛС при приёме фотонного импульса в конце интервала

$$P_{DCR,j} = \exp(-\overline{n_{s,j}} - \overline{n_{DCR,j}}) ; \quad (3.5)$$

– среднее число фотонов в фотонном импульсе при нахождении станции на верхней границе j -го участка

$$\overline{n_{s,j}} = \overline{n_{s0}} \cdot 10^{-\frac{\alpha_{OF}[\text{дБ/км}] \cdot L_j[\text{км}]}{10}} ; \quad (3.6)$$

– вероятность регистрации хотя бы одного фотона или ИТТ во время приёма фотонного импульса при анализе j -го участка

$$P_{Ds,j} = 1 - \exp(-\overline{n_{s,j}} - \xi_{DCR} \cdot \tau_s) ; \quad (3.7)$$

– наименьшее среднее число регистрируемых фотонов и ИТТ на верхней границе j -го участка (нижней границе $(j+1)$ -го участка)

$$\overline{n_{strob,j}} = \overline{n_{s,j}} + \xi_{DCR} \cdot \tau_{strob} ; \quad (3.8)$$

– длительность импульса стробирования с учётом временного отклонения момента прихода фотона вследствие наличия в ОВ дисперсии τ_{OF} [92]:

$$\tau_{strob} = 2 \cdot \tau_s + 2 \cdot \Delta T_s + \tau_{OF} , \quad (3.9)$$

где ΔT_s – нестабильность периода следования синхроимпульсов.

Из выражения (3.1) следует, что для минимизации вероятности ошибки сигнализации необходимо максимизировать вероятность обнаружения на этапе поиска $P_{D,j}$ и минимизировать вероятность ошибки тестирования $P_{err.test,j}$.

Увеличивая количество тестов $N_{test,j}$, как следует из формулы (3.3), можно обеспечить требуемую вероятность ошибки тестирования $P_{err.test,j}$ за время всех допустимых тестов при анализе j -го участка ВОЛС. При этом количество тестов $N_{test,j}$ должно удовлетворять условию

$$N_{test.j} \geq N_{test.min.j} = \left\lceil \frac{1}{\overline{n_{strob.j}}} \cdot \ln \left(\frac{1}{P_{err.test.j}} \right) \right\rceil ,$$

где $[E]$ – наименьшее целое число, превышающее E .

В системах КРК стремятся обеспечить равенство вероятностей ошибки тестирования при анализе любого участка $P_{err.test.j} = P_{err.test.0}$. Кроме того, выполняется условие $\xi_{DCR}\tau_s \ll \overline{n_s}$. Тогда

$$N_{test.j} \geq \left\lceil \frac{1}{\overline{n_{s.j}}} \cdot \ln \left(\frac{1}{P_{err.test.0}} \right) \right\rceil . \quad (3.10)$$

С другой стороны, как следует из (3.1), постоянный рост числа допустимых тестов не приводит к сколь угодно значимому снижению вероятности ошибки синхронизации.

Как следует из (3.2), добиться сколь угодно близкой к 1 вероятности обнаружения фотонного импульса на этапе поиска, увеличивая число анализируемых кадров, невозможно. Максимальная вероятность обнаружения фотонного импульса на этапе поиска в j -м участке ограничена значением

$$P_{D.max.j} = \frac{1 - \exp(-\overline{n_{DCR.j}})}{\overline{n_{DCR.j}}} \cdot \frac{P_{D.s.j}}{1 - P_{DCR.j}} . \quad (3.11)$$

Причём

$$P_{D.j} = P_{D.max.j} \cdot (1 - P_{DCR.j}^{N_j}) . \quad (3.12)$$

С практической точки зрения на верхней границе всех участков должны выполняться условия $P_{err.j} = P_{err.0}$. Откуда с учётом $P_{err.test.j} = P_{err.test.0}$ имеем $P_{D.j} = P_{D.0}$. Тогда из (3.1) следует, что вероятность обнаружения фотонного импульса на этапе поиска за N_j временных кадров на верхних границах всех участков постоянна и равна

$$P_{D.0} = \frac{1 - P_{err.0}}{1 - P_{err.test.0}} . \quad (3.13)$$

Из (3.1) следует, что выполнение условия $K_{test} = P_{err.0}/P_{err.test.0} \gg 1$ снижает влияние этапа тестирования на вероятность ошибки синхронизации. При этом

$$P_{err.test.0} = P_{err.0}/K_{test} . \quad (3.14)$$

Например, при задании отношения вероятностей ошибки синхронизации и тестирования $K_{test}=2$ для обеспечения вероятности ошибки синхронизации $P_{err.0}=0,1$ необходимо иметь $P_{err.test.0}=0,05$. При этом согласно (3.13) вероятность обнаружения фотонного импульса на этапе поиска на верхних границах всех участков должна превышать $P_{D.0}=0,947$. Отметим, что при отсутствии ограничений на предельное число тестов предельная вероятность обнаружения фотонного импульса на этапе поиска составляет 0,9, требуя меньшего числа кадров для обеспечения требуемой вероятности ошибки синхронизации $P_{err.0}=0,1$.

Увеличим отношение вероятностей ошибки синхронизации и тестирования до $K_{test}=10$ при требовании $P_{err.0}=0,1$. Тогда необходимо иметь $P_{err.test.0}=0,01$ и $P_{D.0}=0,909$. Видно, что при выборе $K_{test}=10$ практически исключается влияние этапа тестирования на вероятности ошибки синхронизации (менее 1 %).

Введём коэффициент $K_{D.j} = (1 - P_{D.0}) / (1 - P_{D.max.j})$, отражающий снижение способности обнаружения синхроимпульса из-за ограничения числа анализируемых временных кадров N_j в j -м участке. Тогда требуется обеспечить максимальную вероятность обнаружения фотонного импульса на этапе поиска в j -м участке

$$P_{D.max.j} = 1 - \frac{1 - P_{D.0}}{K_{D.j}}.$$

При равенстве коэффициентов $K_{D.j} = K_D$ и постоянстве $P_{D.max.j} = P_{D.max.0}$ для всех участков $j = \overline{1, N_{FOL}}$ имеем

$$P_{D.max.0} = 1 - \frac{1 - P_{D.0}}{K_D}. \quad (3.15)$$

С учётом (3.12) – (3.15) находим, что предельное число анализируемых кадров должно удовлетворять условию

$$N_j \geq N_{min.j} = \left\lceil \frac{\ln(1 - P_{D.0}/P_{D.max.0})}{\ln(P_{DCR.j})} \right\rceil. \quad (3.16)$$

Из (3.10) и (3.16) следует требование увеличения с ростом номера участка количества анализируемых временных кадров и тестов для гарантирования на

заданном уровне вероятности обнаружения фотонного импульса на этапе поиска и вероятности ошибки тестирования.

Резюме. Получены аналитические выражения для расчёта вероятностных характеристик двухэтапного временного алгоритма синхронизации. Определены соотношения для числа кадров, допустимых на этапе поиска, и числа тестов, допустимых на этапе тестирования.

3.2 Особенности разбиения волоконно-оптической линии на участки с убывающей длиной

Идея разбиения ВОЛС на участки состоит в том, чтобы вероятность ошибки синхронизации на верхней границе любого участка не превышала допустимого значения $P_{err.0}$ [23]. Последнее требует обеспечения максимальной вероятности обнаружения фотонного импульса на этапе поиска в j -м участке, определяемой формулой (3.15). С другой стороны, с учётом условий $\overline{n_{DCR.j}} \ll 1, \overline{n_{s.j}} \ll 1, P_{DCR.j} \cong 1 - \overline{n_{s.j}} - \overline{n_{DCR.j}}$ и $P_{Ds.j} \cong \overline{n_{s.j}}$ формула (3.11) преобразуется к виду

$$P_{D.max.0} = \frac{1 - \exp(-\overline{n_{DCR.j}})}{\overline{n_{DCR.j}}} \cdot \frac{P_{Ds.j}}{1 - P_{DCR.j}} \approx \frac{\overline{n_{s.j}}}{\overline{n_{s.j}} + \overline{n_{DCR.j}}}.$$

Следовательно, на верхней границе любого j -го участка ВОЛС должно выполняться условие

$$\overline{n_{s.j}} \geq \frac{P_{D.max.0}}{1 - P_{D.max.0}} \cdot \overline{n_{DCR.j}}.$$

Используя (2.4) и (3.4), для j -го участка ВОЛС находим

$$\overline{n_{DCR.j}} = \xi_{DCR} \cdot \tau_{lj} = 2 \cdot \xi_{DCR} \cdot l_j / v_{OF} = 2 \cdot \xi_{DCR} \cdot (L_j - L_{j-1}) / v_{OF}.$$

Тогда с учётом (3.6) на верхней границе любого j -го участка ВОЛС должно выполняться условие

$$\overline{n_{s0}} \cdot 10^{-\frac{\alpha_{OF}[\text{дБ/км}] \cdot L_j[\text{км}]}{10}} \geq \frac{P_{D.max.0}}{1 - P_{D.max.0}} \cdot \frac{2 \cdot \xi_{DCR}}{v_{OF}} \cdot (L_j - L_{j-1}). \quad (3.17)$$

Заметим, что предельная длина первого участка ВОЛС при использовании оптического волокна без потерь ($\alpha_{OF}=0$ дБ/км) определяется формулой

$$l_{lim} = \frac{\overline{n_{s0}} \cdot v_{OF}}{2 \cdot \xi_{DCR}} \cdot \frac{1 - P_{D.max.0}}{P_{D.max.0}}. \quad (3.18)$$

Видно, что предельная длина первого участка прямо пропорционально среднему числу фотонов за длительность оптического импульса на выходе из кодирующей станции и обратно пропорционально частоте генерации ИТТ в фотодетекторе. Отметим, что предельная длина первого участка ВОЛС l_{lim} соответствует предельной протяжённости ВОЛС в алгоритме-аналоге при использовании оптического волокна без потерь.

На рисунке 3.1 представлены зависимости предельной протяжённости ВОЛС l_{lim} от частоты генерации ИТТ в фотодетекторе ξ_{DCR} при 4-х значениях допустимой вероятности ошибки синхронизации на верхней границе любого участка $P_{err.0}$ (0,01; 0,02; 0,05 и 0,10).

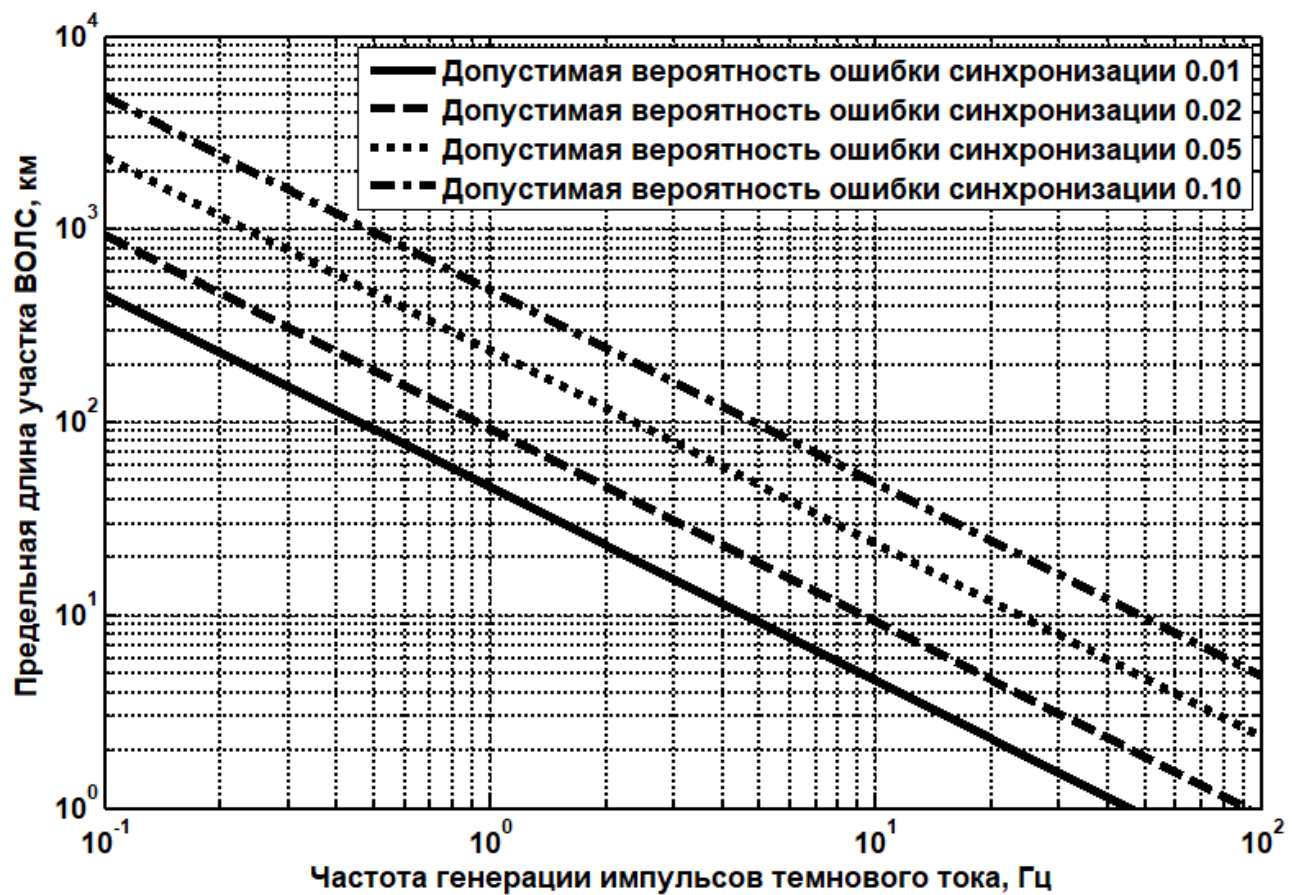


Рисунок 3.1 – Зависимости предельной длины первого участка ВОЛС от частоты генерации ИТТ в фотодетекторе

В расчётах принято, что станции соединены одномодовым ОВ Corning® SMF-28 с погонным затуханием 0,18 дБ/км на длине волны 1550 нм. Показатель преломления оптического излучения в сердцевине волокна $n_{OF}=1,4682$ определяет скорость распространения фотонов $v_{OF}=204\,332$ км/с. Среднее число фотонов за длительность импульса на выходе кодирующей станции равно $\overline{n_{s0}}=0,1$.

Диапазон частот генерации ИТТ $\xi_{DCR} = 0,1 \dots 100$ Гц характерен для однофотонных лавинных фотодиодов (ID-201 – $0,1 \dots 100$ Гц [106]; ID-210 – $0,4 \dots 8$ Гц [107]; ID-230 – $50 \dots 80$ Гц [108]; ID-280 и ID-281 – $1 \dots 100$ Гц [109]). В расчётах принято $K_{test}=10$ и $K_D=2$.

Отметим, что заданным вероятностям ошибки синхронизации на верхней границе $P_{err.0}$ 0,01; 0,02; 0,05 и 0,10 соответствуют допустимые вероятности ошибки тестирования $P_{err.test.0}$ 0,001; 0,002; 0,005 и 0,010 и допустимые вероятности обнаружения на этапе поиска $P_{D.0}$ 0,9910; 0,9820; 0,9548 и 0,9091. При этом максимальная вероятность обнаружения на этапе поиска $P_{D.max.0}$ соответственно равна 0,9955; 0,9910; 0,9774 и 0,9545.

Графики на рисунке 3.1 доказывают, что в аналоге даже при использовании ОВ без потерь предельная дальность не превышает 100 км при требовании допустимой вероятности ошибки синхронизации не выше 0,02 и выборе ОЛФД с частотой генерации ИТТ не более 1 Гц. Кроме того, из графиков следует, что внедрение алгоритма синхронизации, предполагающего последовательный временной анализ участков с убывающей длиной, позволит использовать ОЛФД с худшими шумовыми свойствами. Естественно, что это позволит снизить стоимость аппаратуры.

Применяя строгое равенство в (3.17) с учётом (3.18), получаем трансцендентное уравнение для определения верхней границы j -го участка L_j при известной верхней границе $(j-1)$ -го участка L_{j-1} :

$$L_j = \begin{cases} l_{lim} \cdot 10^{-\frac{\alpha_{OF} \left[\frac{дБ}{км} \right] \cdot L_1 [км]}{10}}, & j = 1; \\ L_{j-1} + l_{lim} \cdot 10^{-\frac{\alpha_{OF} \left[\frac{дБ}{км} \right] \cdot L_j [км]}{10}}, & j \geq 2. \end{cases} \quad (3.19)$$

Полученные соотношения и условия позволяют скорректировать методику разбиения волоконно-оптической линии на участки с убывающей длиной, описанную в [23]. Главное отличие состоит в том, что ранее методика строилась исходя из допустимого ухудшения вероятности обнаружения фотонного импульса

из-за ограничения числа анализируемых кадров на этапе поиска в j -м участке. Требования же к вероятности ошибки синхронизации не предъявлялось.

Приступая к разбиению волоконно-оптической линии на участки, задаётся погонное затухание α_{OF} и показатель преломления сердцевины n_{OF} оптического волокна, частота генерации ИТТ в ОЛФД ξ_{DCR} , среднее число фотонов $\overline{n_{s0}}$ за длительность оптического импульса на выходе из кодирующей станции и допустимая вероятность ошибки синхронизации $P_{err.0}$.

Задаётся вероятность ошибки тестирования $P_{err.test.0}$, которая фиксирована для любого участка. Возможно задание коэффициента K_{test} , определяющего влияние этапа тестирования на ошибку синхронизации. После, используя (3.14), находится вероятность ошибки тестирования $P_{err.test.0}$.

Используя формулу (3.13), рассчитывается вероятность обнаружения фотонного импульса на этапе поиска на верхних границах участков $P_{D.0}$. Задаётся коэффициент K_D и по формуле (3.15) находится максимальная вероятность обнаружения фотонного импульса на этапе поиска в участке $P_{D.max.0}$, которая требуется для обеспечения рассчитанной вероятности $P_{D.0}$.

По формуле (2.1) рассчитывается скорость распространения фотона в ОВ v_{OF} . Определяется по (3.18) предельная длина участка ВОЛС l_{lim} . В соответствии с трансцендентными уравнениями (3.19) находятся верхние границы участков L_j .

Длина j -го участка определяется по формуле (2.3). Время анализа каждого участка рассчитывается по формуле (2.4).

Результаты расчётов по описанной методике представлены в таблице 3.1. Расчёты выполнены для синхронизации с последовательным опросом 10-ти участков ВОЛС на основе одномодового ОВ Corning SMF-28e. Последнее определяет скорость распространения оптического излучения в сердцевине $v_{OF}=204\,332$ км/с. Частота генерации ИТТ принята равной $\xi_{DCR}=6$ Гц [107], что соответствует применению ОЛФД id210-SFM-C (Standard) при квантовой эффективности фотокатода 10 %. Среднее число фотонов в фотонном импульсе на выходе кодирующей станции – $\overline{n_{s0}}=0,1$. При расчётах принято $K_{test}=10$ и $K_D=2$.

Неточность расчётов границ участков в соответствии с трансцендентными уравнениями (3.19) находится в пределах 0,05 ... 0,10 %.

Данные таблицы 3.1 позволяют выбрать общую протяжённость ВОЛС, на которой гарантируется синхронизация с заданной вероятностью ошибки. Например, разбиение ВОЛС на 10 участков гарантирует синхронизацию с вероятностью ошибки 0,01 при разнесении станций на 33,4 км.

Из таблицы 3.1 видно, что если в алгоритме-прототипе подсистема синхронизации с вероятностью ошибки не выше 0,02 может работать при протяжённости ВОЛС не более 10,2 км, то в предлагаемом алгоритме при разбиении ВОЛС на 10 участков – свыше 46 км. Возможное разнесение станций увеличивается в 4,5 раза. Отметим, что предельная длина участка ВОЛС при использовании ОВ без потерь ($\alpha_{OF}=0$ дБ/км), рассчитанная по (3.18), составляет 18,6 км.

Таблица 3.1 – Верхние границы участков ВОЛС, км

$P_{err.0}$	$l_{lim},$ км	Номер участка									
		1	2	3	4	5	6	7	8	9	10
0,01	9,3	6,0	10,9	15,0	18,6	21,7	24,5	27,0	29,3	31,4	33,4
0,02	18,6	10,2	17,6	23,5	28,3	32,4	35,9	38,9	41,7	44,2	46,4
0,05	23,6	18,4	29,8	38,0	44,3	49,4	53,6	57,3	60,5	63,4	65,9
0,10	48,7	26,8	41,3	51,1	58,3	64,1	68,7	72,7	76,2	79,2	82,0

Важно, что длина десяти участков превышает предельную длину участка ВОЛС при использовании ОВ без потерь в 3,6 раза при $P_{err.lim}=0,01$ и в 1,7 раза при $P_{err.lim}=0,1$.

В первом приближении можно считать, что увеличение требуемого числа участков обратно пропорционально снижению вероятности ошибки синхронизации при фиксированном разнесении станций.

Особенности изменения длины участков поясняют данные таблицы 3.2. Как и следовало ожидать, с ростом номера участка его длина уменьшается. Так, например, при допустимой вероятности ошибки 0,1 различие в длине 1-го и 10-го участков достигает почти 10 раз. Причём, при допустимой вероятности ошибки 0,1 длина 1-го участка равна 26,75 км, 5-го – 5,72 км, а 10-го – всего 2,73 км. Различие между длинами 1-го и 2-го участков превышает 1,8 раза и уже 11 % между 9-м и

10-м участками. Последнее указывает, что применение предлагаемого однофотонного алгоритма синхронизации станций с последовательным опросом участков с убывающей длиной также имеет ограничение по протяжённости ВОЛС.

Таблица 3.2 – Длина участков ВОЛС, км

$P_{err.0}$	Номер участка									
	1	2	3	4	5	6	7	8	9	10
0,01	6,01	4,90	4,13	3,56	3,14	2,79	2,51	2,28	2,09	1,94
0,02	10,17	7,47	5,85	4,80	4,07	3,50	3,07	2,77	2,50	2,25
0,05	18,38	11,44	8,17	6,29	5,10	4,25	3,67	3,21	2,87	2,56
0,10	26,75	14,59	9,76	7,23	5,72	4,69	3,98	3,46	3,05	2,73

Действительно, минимальная длина анализируемого участка не должна быть меньше удвоенного расстояния, на которое может переместиться фотон за длительность импульса. Следовательно, $L_j - L_{j-1} \geq 2 \cdot v_{OF} \cdot \tau_s$. Применяя строгое равенство с учётом (3.19), находим предельное разнесение станций, на котором возможна синхронизация с заданной вероятностью ошибки

$$L_{lim} = \frac{10}{\alpha_{OF} \left[\frac{\text{дБ}}{\text{км}} \right]} \cdot \lg \left(\frac{l_{lim}}{2 \cdot v_{OF} \cdot \tau_s} \right). \quad (3.20)$$

Например, при допустимой вероятности ошибки синхронизации 0,01, $l_{lim}=9,3$ км и длительности лазерного импульса $\tau_s=300$ пс находим, что разнесение станций не может быть более 271 км (без учёта дисперсионных свойств ОВ).

Данные таблицы 3.3 позволяют проследить изменение параметров синхронизации с однофотонным ЛФД id210-SFM-C (Standard) на границах десяти участков ВОЛС на основе одномодового ОВ Corning SMF-28e. Частота генерации ИТТ принята равной $\xi_{DCR}=6$ Гц. При расчётах принято $\overline{n_{s0}}=0,1$; $P_{err.0}=0,01$; $P_{err.test.0}=0,001$; $P_{D.0}=0,991$; $P_{D.max.0}=0,9955$.

Из таблицы видно, что отношение среднего числа фотонов на верхней границе участков к среднему числу ИТТ за время анализа участка (последний столбец в таблице 3.3) различается менее чем на 1 %. Вариации отношения связаны с неточностью расчёта верхних границ участков (в примере 0,1 %) в соответствии с трансцендентным уравнением (3.19).

Таблица 3.3 – Параметры подсистемы синхронизации

Номер участка j	Параметр участка волоконно-оптической линии					
	Верхняя граница участка, км	Длина участка, км	$\tau_{L,j}$, мкс	$\overline{n_{sj}}$	$\overline{n_{DCR,j}}$	$\frac{\overline{n_{sj}}}{\overline{n_{DCR,j}}}$
1	6,01	6,01	58,79	0,0780	$3,53 \cdot 10^{-4}$	221,02
2	10,91	4,90	47,98	0,0636	$2,88 \cdot 10^{-4}$	221,02
3	15,04	4,13	40,43	0,0536	$2,43 \cdot 10^{-4}$	221,01
4	18,60	3,56	34,84	0,0463	$2,09 \cdot 10^{-4}$	221,34
5	21,74	3,14	30,71	0,0406	$1,84 \cdot 10^{-4}$	220,45
6	24,53	2,79	27,32	0,0362	$1,64 \cdot 10^{-4}$	220,71
7	27,03	2,51	24,52	0,0326	$1,47 \cdot 10^{-4}$	221,65
8	29,31	2,28	22,32	0,0297	$1,34 \cdot 10^{-4}$	221,63
9	31,40	2,09	20,47	0,0272	$1,23 \cdot 10^{-4}$	221,50
10	33,35	1,94	19,00	0,0251	$1,14 \cdot 10^{-4}$	220,22

Благодаря постоянству отношения сигнал/шум на верхних границах участков гарантируется вероятность ошибки синхронизации не хуже заданного значения в пределах любого участка.

Время на однократный просмотр всех участков ВОЛС τ_{FOL} не может превышать значение периода следования фотонных импульсов T_s . На практике же выполняется строгое неравенство (см. рисунок 2.1)

$$\tau_{FOL} = \sum_{j=1}^{N_{FOL}} \tau_{l_j} < T_s.$$

При ориентации на предельно-возможное разнесение L_{FOL} станций автокомпенсационной системы КРК период следования оптических синхроимпульсов должен удовлетворять условию (2.5). Следовательно, частота следования лазерных синхроимпульсов не может превышать значения

$$f_s = \frac{1}{T_s} < \frac{v_{OF}}{2 \cdot L_{FOL.max}}. \quad (3.21)$$

В таблице 3.4 представлены результаты расчётов по формулам (2.1), (2.5) и (3.21) для ВОЛС на основе одномодового (Corning[®] SMF-28e) и многомодовых (InfiniCor 50 и InfiniCor 62.5) ОВ с разными эффективными показателями преломления сердцевины n_{OF} для излучения с различными длинами волн. Поскольку отличие эффективных показателей преломления сердцевины и скорости

распространения фотона для разных ОВ при разных длинах волн излучения невелико, то и частоты следования лазерных синхроимпульсов различаются не более чем на 2 %. Последнее позволяет для выбора частоты следования лазерных импульсов при выполнении условия $T_s > (1,02 \dots 1,05) \cdot \tau_{FOL}$ для синхронизации разнесённых на L_{FOL} станций использовать приближённую формулу

$$f_s [\text{кГц}] < 100/L_{FOL} [\text{км}].$$

Таблица 3.4 – Зависимость частоты следования оптических синхроимпульсов от разнесения станций в системе КРК (в килогерцах)

Оптическое волокно; эффективный показатель преломления сердцевины, длина волны излучения	Предельно-возможное разнесение станций, км						
	1	2	5	10	20	50	100
Corning SMF-28e; 1,46820; 1550 нм	102,17	51,08	20,43	10,22	5,11	2,04	1,02
Corning SMF-28e; 1,4677; 1310 нм	102,20	51,10	20,44	10,22	5,11	2,04	1,02
InfiniCor 50; 1,481; 850 нм	101,28	50,64	20,26	10,13	5,06	2,03	1,01
InfiniCor 50; 1,476; 1300 нм	101,63	50,81	20,33	10,16	5,08	2,03	1,02
InfiniCor 62.5; 1,496; 850 нм	100,27	50,13	20,05	10,03	5,01	2,00	1,00
InfiniCor 62.5; 1,491; 1300 нм	100,60	50,30	20,12	10,06	5,03	2,01	1,01

Из таблицы 3.4 видно, что для автокомпенсационной системы КРК при защите локальных волоконно-оптических сетей с дальностью квантовых каналов до 1 км частота следования оптических синхроимпульсов может составлять 100 кГц. Однако при защите городских и региональных волоконно-оптических сетей с дальностью квантовых каналов свыше 1 км при априорно известном значении только предельно-возможного разнесения станций $L_{FOL} > 10$ км частота следования синхроимпульсов не превышает 10 кГц.

Исследование зависимости между вероятностью ошибки синхронизации и разнесением станций. Результаты расчётов по формуле (3.1) вероятности ошибки синхронизации представлены на рисунке 3.2 при частоте генерации ИТТ 6 Гц при разных допустимых вероятностях ошибки синхронизации $P_{err.0}=0,01$; 0,02; 0,05; 0,10 (соответственно сплошная, штриховая, пунктирная и штрихпунктирная линии). Среднее число фотонов за длительность импульса на выходе кодирующей станции равно $\overline{n_{s0}}=0,1$.

Скачкообразные изменения функции соответствуют переходам к анализу следующего участка ВОЛС. На верхних границах каждого участка обеспечивается заданная вероятность ошибки синхронизации. Отличие от требуемой допустимой вероятности не превышает 2...3 %.

Особенности предлагаемого алгоритма синхронизации поясняются графиками на рисунке 3.3, построенными при $P_{err,0}=0,01$. Здесь сплошной линией показаны изменения среднего числа принимаемых фотонов, а штриховой линией – среднего числа импульсов ИТТ за время стробирования.

Видно скачкообразное изменение среднего числа импульсов ИТТ за счёт сокращения времени анализа каждого последующего участка ВОЛС. Действительно, при переходе от 1-го участка к 2-му среднее число импульсов ИТТ за время анализа падает с $1,6 \cdot 10^{-3}$ до $8,2 \cdot 10^{-4}$ (в 1,9 раза), а при переходе от 2-го участка к 3-му – с $8,2 \cdot 10^{-4}$ до $5,4 \cdot 10^{-4}$ (в 1,5 раза). Такое же скачкообразное изменение характерно и для отношения средних чисел принимаемых фотонов и ИТТ: оно максимально в начале и минимально в конце каждого участка.



Рисунок 3.2 – Вероятность ошибки синхронизации

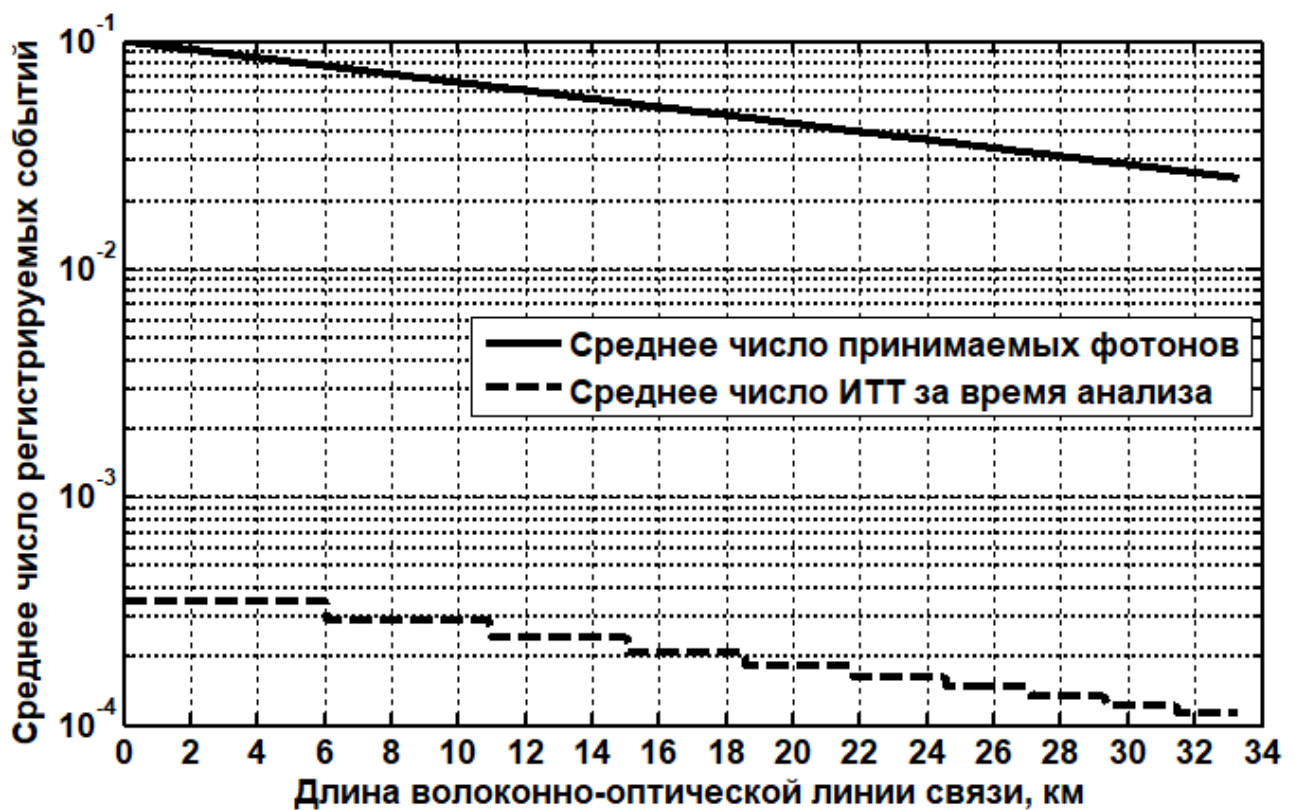


Рисунок 3.3 – Среднее число принимаемых фотонов и ИТТ за время анализа

Важно, что в пределах участка среднее число импульсов ИТТ постоянно. А вот среднее число принимаемых фотонов падает монотонно в пределах любого участка ВОЛС. При этом отношение средних чисел принимаемых фотонов и ИТТ в конце всех участков равно ~ 220 (см. последний столбец данных в таблице 3.3). Благодаря этому вероятности ошибки синхронизации в конце всех участков одинаковы, совпадая с заданным допустимым значением.

Различие вероятностей ошибки синхронизации в начале и в конце участка уменьшается с ростом номера участка. Например, отношение вероятностей в 1-м участке ВОЛС при $P_{err.0}=0,01$ равно 2,2 раза, в то время как в 10-м участке составляет 1,3 раза.

Зависимости вероятности ошибки синхронизации от протяжённости ВОЛС для случая применения ОЛФД ID-230 с частотой генерации ИТТ 50 Гц представлены на рисунке 3.4 для 4-х вероятностей ошибки синхронизации $P_{err.0}$.

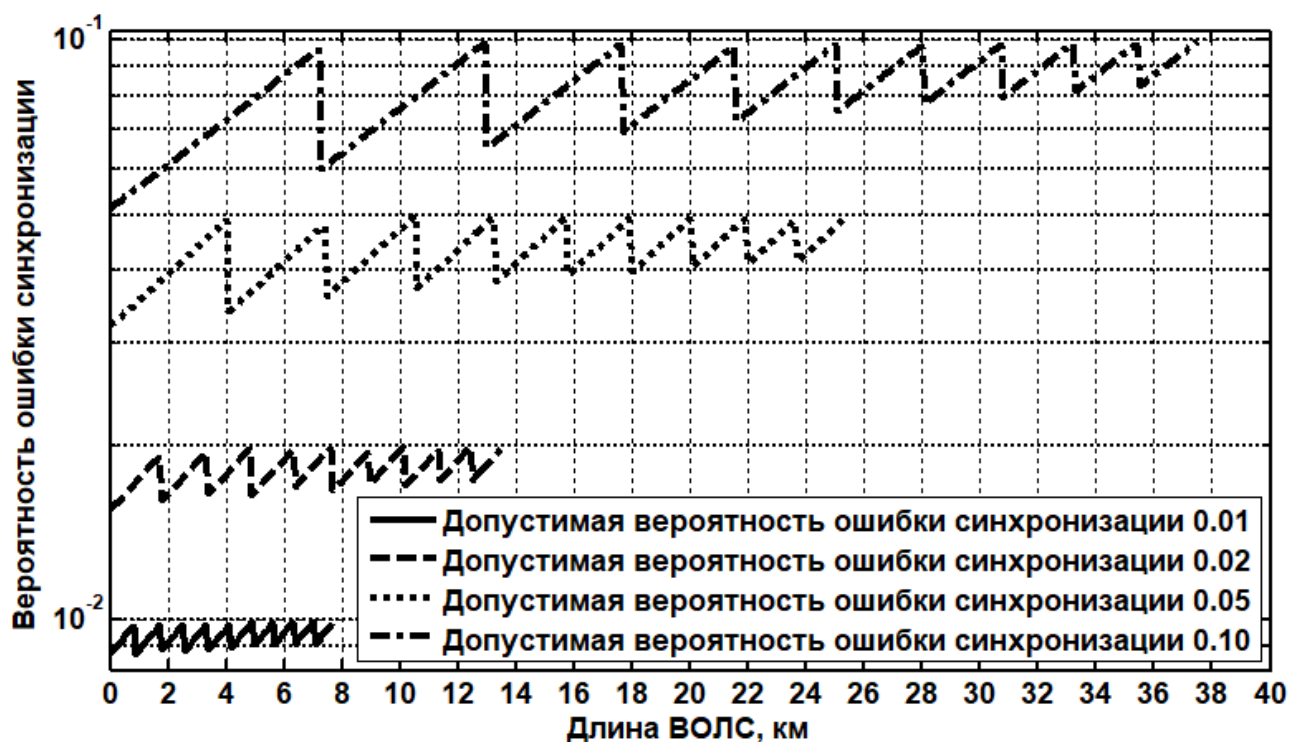


Рисунок 3.4 – Зависимости вероятности ошибки синхронизации от протяжённости ВОЛС

Сравнение с графиками на рисунке 3.2 показывает, что с ростом частоты генерации ИТТ разброс вероятностей ошибки синхронизации в пределах любого участка заметно сокращается. Например, в 1-м участке при $P_{err.0}=0,01$ разброс равен 1,11 раза по сравнению с 2,2 раза при $\xi_{DCR}=6$ Гц.

Таблица 3.5 – Протяжённость ВОЛС (в километрах)

$P_{err.0}$	ID-201 $\xi_{DCR}=0,1$ Гц	ID-210 $\xi_{DCR}=6$ Гц	ID-230 $\xi_{DCR}=50$ Гц	ID-280 $\xi_{DCR}=100$ Гц
0,01	122,13	33,35	7,72	4,19
0,02	138,57	46,44	13,50	7,75
0,05	160,61	65,94	25,35	16,09
0,10	177,83	81,96	37,53	25,78

Как и следовало ожидать с ростом частоты генерации ИТТ значительно уменьшается разнесение станций при заданной вероятности ошибки синхронизации. Результаты расчётов разнесения станций при использовании однофотонных ЛФД с разными частотами генерации ИТТ сведены в таблицу 3.5. Увеличение частоты генерации ИТТ в ~ 10 раз (с 6 до 50 Гц) при гарантии вероятности ошибки синхронизации $P_{err.0}=0,1$ приводит к сокращению длины ВОЛС в 2,2 раза. Ещё более значительные ограничения на разнесение станций

наблюдаются при ужесточении требований к вероятности ошибки синхронизации (при $P_{err.0}=0,01$ сокращение длины ВОЛС в 4,3 раза).

Резюме. Предложена методика разбиения ВОЛС на участки с убывающей длиной, причём длина каждого последующего участка меньше длины предыдущего участка. Последнее позволяет значительно уменьшить влияние ИТТ ОЛФД за время анализа участка. Благодаря этому увеличивается отношение сигнал/шум. Отмечена связь между вероятностью ошибки синхронизации и разнесением станций. С ужесточением требований к вероятности ошибки синхронизации протяженность линии, соединяющей станции, уменьшается в разы.

3.3 Схемотехнические решения для опроса участков ВОЛС с убывающей длиной

Синхронизация станций в предлагаемом алгоритме проходит в два этапа: этап поиска фотона во временном интервале, определяемом анализируемым участком ВОЛС, и этап тестирования для подтверждения приёма фотонного импульса.

Исходя из постоянства вероятностей ошибки тестирования при анализе любого участка $P_{err.test.j} = P_{err.test.0}$, формулируются требования (3.10) к количеству тестов $N_{test.j}$ при анализе j -го участка ВОЛС. С практической стороны для реализации управления в цифровой форме важно, чтобы это число было кратно двум. Следовательно, дополнительно к (3.10) должно выполняться условие $N_{test.j} = 2^{k_{test.j}}$. Откуда разрядность цифрового блока управления для контроля допустимого числа тестирований определяется формулой

$$k_{test.j} \geq \left\lceil \log \left[\frac{1}{n_{s,j}} \cdot \ln \left(\frac{1}{P_{err.test.0}} \right) \right] \right\rceil. \quad (3.22)$$

В таблице 3.6 представлены результаты расчётов разрядности цифрового блока управления тестированием и допустимого числа тестов при вероятности ошибки тестирования $P_{err.test.0}=0,01$ для 4-х значений допустимой вероятности ошибки синхронизации.

Платой за цифровую реализацию блока управления для контроля допустимого числа тестирований является увеличение допустимого числа тестов, а, следовательно, и времени тестирования. Например, расчёт при вероятности ошибки синхронизации 0,02 для 5-го участка даёт предельное число тестов в 238, то при цифровой реализации уже 256 (увеличение порядка 8 %).

Таблица 3.6 – Число тестов/разрядность цифрового блока управления для контроля допустимого числа тестирований

$P_{err.lim}$	Номер участка									
	1	2	3	4	5	6	7	8	9	10
0,01	$\frac{128}{7}$	$\frac{128}{7}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{512}{9}$
0,02	$\frac{128}{7}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$
0,05	$\frac{128}{7}$	$\frac{256}{8}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{1024}{10}$	$\frac{1024}{10}$	$\frac{1024}{10}$	$\frac{1024}{10}$
0,10	$\frac{256}{8}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{1024}{10}$	$\frac{1024}{10}$	$\frac{1024}{10}$	$\frac{1024}{10}$	$\frac{2048}{11}$	$\frac{2048}{11}$	$\frac{2048}{11}$

В ряде случаев расхождение значительно (до 2-х раз). Например, это проявляется при анализе 3-го участка при $P_{err.0}=0,01$, где расхождение составляет 98% (129 против 256). В этом случае целесообразно рассмотреть возможность использовать меньшую на одну позицию разрядность цифрового блока. Так если в предшествующем примере оставить разрядность для 3-го участка такой же, как и для 2-го (разрядность 7), то расхождение составит только 0,8 % (причём в сторону уменьшения времени тестирования). Однако при этом изменится (несколько ухудшится) вероятность ошибки тестирования.

Аналогично, исходя из требования $N_j = 2^{k_j}$ при постоянстве коэффициентов $K_{D,j} = P_{D.max,j}/P_{D,j} = K_D$ для любого участка, условие (3.11) преобразуется к виду:

$$k_j \geq \left\lceil \log \left[\frac{1}{\ln(P_{DCR,j})} \cdot \ln \left(1 - \frac{P_{D,0}}{P_{D.max,0}} \right) \right] \right\rceil. \quad (3.23)$$

В таблице 3.7 представлены результаты расчётов разрядности цифрового блока управления поиском и допустимого числа анализируемых кадров для коэффициента $K_D=2$, отражающего снижение способности обнаружения синхроимпульса из-за ограничения числа анализируемых временных кадров.

Таблица 3.7 – Предельное число анализируемых кадров/разрядность цифрового блока управления поиском

$P_{err.0}$	Номер участка									
	1	2	3	4	5	6	7	8	9	10
0,01	$\frac{128}{7}$	$\frac{128}{7}$	$\frac{128}{7}$	$\frac{128}{7}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$
0,02	$\frac{128}{7}$	$\frac{128}{7}$	$\frac{128}{7}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$
0,05	$\frac{128}{7}$	$\frac{128}{7}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{1024}{10}$
0,10	$\frac{128}{7}$	$\frac{256}{8}$	$\frac{256}{8}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{512}{9}$	$\frac{1024}{10}$	$\frac{1024}{10}$	$\frac{1024}{10}$	$\frac{1024}{10}$

Как и в случае с расчётом числа тестирований, предельное число анализируемых кадров может быть практически в два раза больше при реализации модуля управления в цифровом виде. Например, в 8-м участке при $P_{err.0}=0,02$ расхождение достигает 95% (263 против 512), в 5-м участке при $P_{err.0}=0,01$ – 92 % (133 против 256). Однако за счёт незначительного увеличения вероятности ошибки тестирования это расхождение можно нивелировать. В подавляющих случаях расхождение минимально. Так, при $P_{err.0}=0,05$ в 9-м и при $P_{err.0}=0,02$ в 3-м участках расхождение составляет 0,4 % и 3 % соответственно.

Резюме. При использовании цифровых технологий для реализации предлагаемого алгоритма возникает необходимость кратности числа кадров и тестов 2. Следовательно, происходит увеличение указанных параметров, что приводит к повышению временных характеристик алгоритма синхронизации.

3.4 Методика расчёта временных и энергетических характеристик двухэтапного временного алгоритма синхронизации

Определим условные временные параметры этапов. Здесь и далее термин «условные» подчёркивает предположение о поиске фотонного импульса в конкретном участке ВОЛС, регистрации фотона или ИТТ в конкретном кадре на этапе поиска или при конкретном тесте на этапе тестирования.

Условные временные параметры этапа поиска при анализе 1-го участка ВОЛС. Аппаратура на этапе поиска регистрирует фотон или ИТТ в интервале

$[0, \tau_{l_1}]$ в первом кадре $[0, T_s]$. Здесь $\tau_{l_1} < T_s$ – временной интервал (сегмент), соответствующий первому участку ВОЛС, длиной $l_1 = L_1$ (рисунок 3.5).

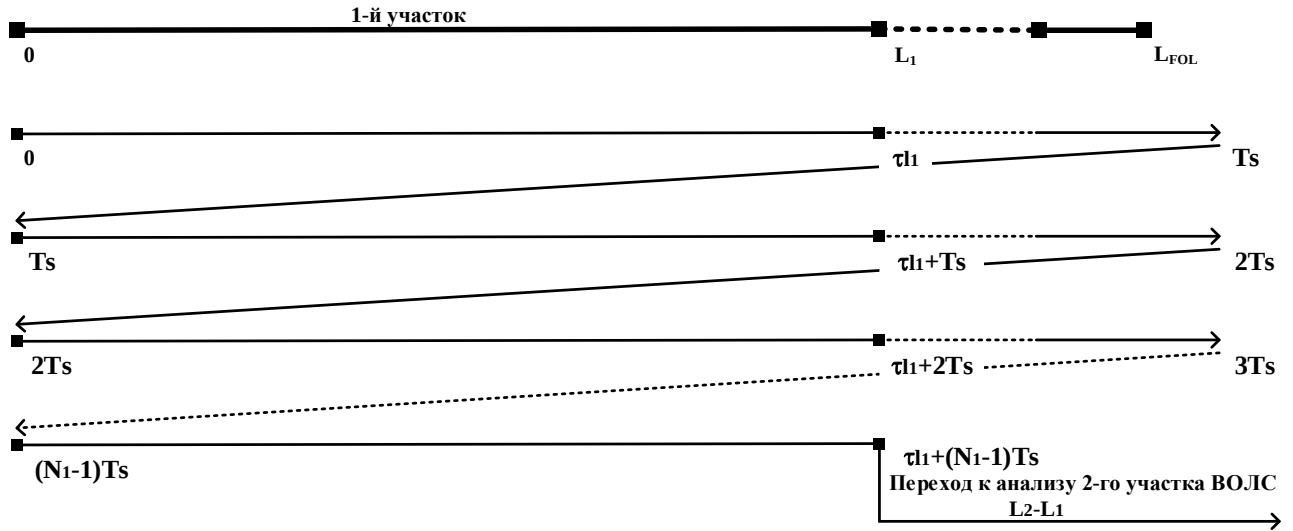


Рисунок 3.5 – Поиск фотона при анализе 1-го участка ВОЛС

Если фотон не зарегистрирован в интервале $[0, \tau_{l_1}]$ первого кадра, то поиск продолжается в интервалах $[(i_{l_1}-1) \cdot T_s, (i_{l_1}-1) \cdot T_s + \tau_{l_1}]$ последующих временных кадров $[(i_{l_1}-1) \cdot T_s, i_{l_1} \cdot T_s]$, $N_1 \geq i_{l_1} > 1$. Здесь через N_1 обозначено предельное число временных кадров, допустимых для анализа 1-го участка ВОЛС.

Если за предельное число временных кадров N_1 не зарегистрирован фотон, то аппаратура переходит к проверке второго участка ВОЛС протяжённостью $l_2 = L_2 - L_1$. В этом случае поиск в 1-м участке ВОЛС будет завершён в момент

$$t_{l_1} = \tau_{l_1} + (N_1 - 1) \cdot T_s. \quad (3.24)$$

Отметим, что для синхронизации станций используется генератор тактовых импульсов, период следования которого равен (или кратен) периоду следования синхроимпульсов. Тогда момент окончания поиска в 1-м участке составит

$$t_{l_1} = N_1 \cdot T_s. \quad (3.25)$$

При регистрации фотона в момент (рисунок 3.6)

$$t_{l_1 s_1} \in [(i_{l_1} - 1) \cdot T_s, (i_{l_1} - 1) \cdot T_s + \tau_{l_1}]$$

в i_{l_1} -м кадре при анализе 1-го участка аппаратура переходит к тестированию, где повторный опрос фотодетектора производится последовательно в интервалах

$$[t_{strob1} + (k_1 - 1) \cdot T_s, t_{strob2} + (k_1 - 1) \cdot T_s], \quad k_1 = \overline{1, N_{test.1}}.$$

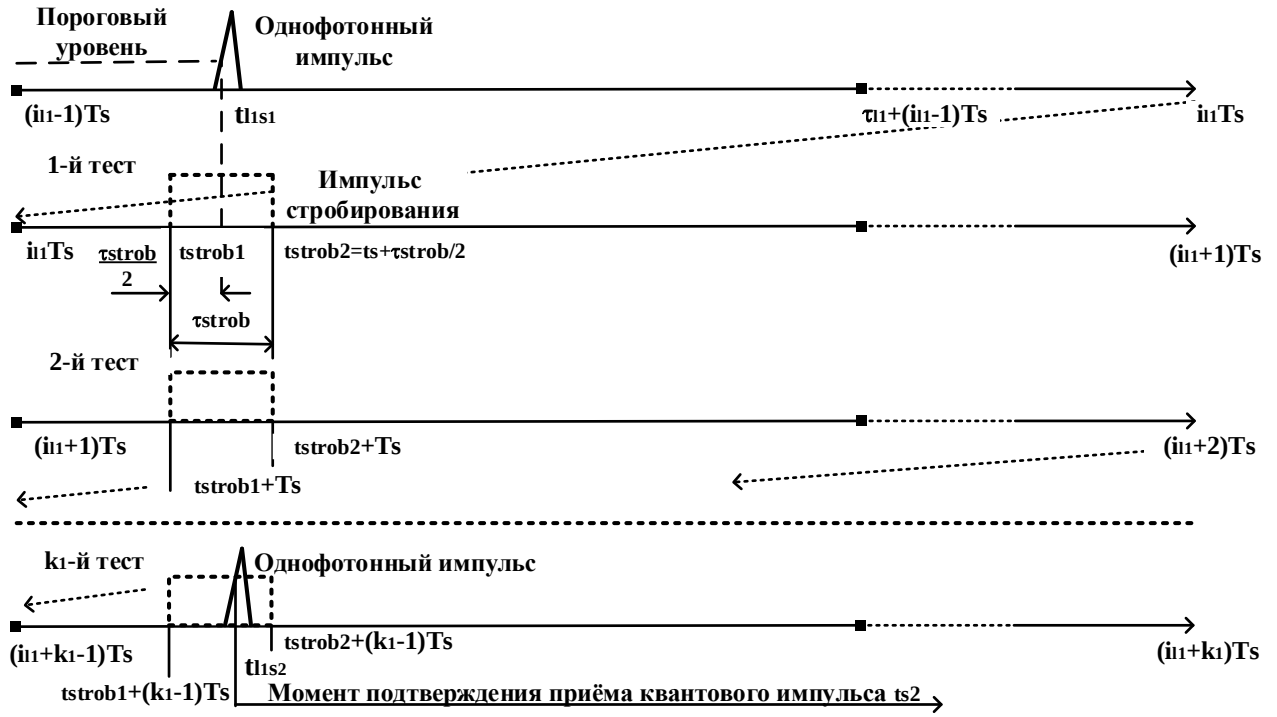


Рисунок 3.6 – Этап тестирования при анализе 1-го участка ВОЛС

С позиций моделирования целесообразно ввести величину

$$x_{l_1s_1} = RNG_{l_1s_1} \cdot \tau_{l_1} = t_{l_1s_1} - (i_{l_1} - 1) \cdot T_s,$$

которая имеет непрерывное равномерное распределение $w(x_{l_1s_1}) = 1/\tau_{l_1}$ на интервале $[0, \tau_{l_1}]$. Причём RNG представляет генератор случайного числа с непрерывным равномерным распределением на интервале $[0, 1]$.

Следовательно, для моделирования момента перехода к этапу тестирования в i_{l_1} -м кадре при анализе 1-го участка ВОЛС $t_{l_1s_1}$ можно использовать формулу

$$t_{l_1s_1} = (i_{l_1} - 1) \cdot T_s + RNG_{l_1s_1} \cdot \tau_{l_1}. \quad (3.26)$$

Условные временные параметры этапа тестирования при анализе 1-го участка ВОЛС. На этапе тестирования повторный опрос фотодетектора производится только в интервалах ожидаемого прихода фотонного импульса во время действия импульса стробирования длительностью τ_{strob} . Отметим, что в остальное время канал однофотонной регистрации не реагирует на приём фотонов и генерацию ИТТ в фотодетекторе.

Установлено, что из-за априорной неопределённости в отношении момента приёма сигнального излучения длительность импульса стробирования τ_{strob} ,

определяемая формулой (3.9), должна превышать длительность оптического синхроимпульса τ_s более чем в 2 раза [92].

Моменту начала действия импульса стробирования во время первого тестирования для подтверждения факта приёма фотонного импульса соответствует

$$t_{l_1strob_1} = t_{l_1s_1} + \Delta\tau + T_s - 0,5 \cdot \tau_{strob} ,$$

а моменту окончания действия импульса стробирования

$$t_{l_1strob_2} = t_{l_1s_1} + \Delta\tau + T_s + 0,5 \cdot \tau_{strob} .$$

Величина $\Delta\tau$ представляет время задержки между моментами приёма и регистрации фотона.

Пусть регистрация фотона в момент $t_{l_1s_2}$ в i_{l_1} -м кадре ($N_1 \geq i_{l_1} \geq 1$) в 1-м участке ВОЛС подтверждена при k_1 -м тестировании ($N_{test.1} \geq k_1 \geq 1$). При этом результирующее время синхронизации является случайной величиной, зависящей от случайного момента регистрации фотона $t_{l_1s_1}$ и случайного номера кадра i_{l_1} на этапе поиска, а также от случайного момента регистрации фотона $t_{l_1s_2}$ и случайного номера теста k_1 на этапе тестирования.

Момент обнаружения фотонного импульса в i_{l_1} -м кадре при k_1 -м тесте 1-го участка ВОЛС определяется формулой

$$t_{l_1D} = t_{l_1s_2} = t_{l_1strob_1} + RNG_{l_1s_2} \cdot \tau_{strob} + (k_1 - 1) \cdot T_s .$$

Следовательно, для моделирования момента обнаружения фотонного импульса в i_{l_1} -м кадре при k_1 -м тесте 1-го участка ВОЛС можно использовать формулу

$$t_{l_1D} = (i_{l_1} + k_1 - 1) \cdot T_s + \Delta\tau - 0,5 \cdot \tau_{strob} + RNG_{l_1s_1} \cdot \tau_{l_1} + RNG_{l_1s_2} \cdot \tau_{strob} . \quad (3.27)$$

Если же за предельное допустимое количество тестов $N_{test.1}$ приём фотона не зафиксирован, то аппаратура вновь возвращается в режим поиска. Момент отрицательного результата тестирования в i_{l_1} -м кадре при последнем $N_{test.1}$ -м тесте 1-го участка ВОЛС может быть определён по формуле

$$t_{l_1ND} = t_{l_1strob_1} + (N_{test.1} - 1) \cdot T_s + \tau_{strob}$$

или

$$t_{l_1ND} = (i_{l_1} + N_{test.1} - 1) \cdot T_s + \Delta\tau + 0,5 \cdot \tau_{strob} + RNG_{l_1s_1} \cdot \tau_{l_1}. \quad (3.28)$$

Если за предельное допустимое количество кадров N_1 на этапе поиска или тестов $N_{test.1}$ на этапе тестирования приём фотона не зафиксирован, то теперь проверяется уже второй участок ВОЛС с протяжённостью l_2 .

Условные временные параметры при анализе 2-го участка ВОЛС. Аппаратура на этапе поиска во 2-м временном сегменте (во 2-м участке ВОЛС) последовательно проверяет наличие фотонного импульса во временных интервалах

$$[t_1 + (i_{l_2} - 1) \cdot T_s + \tau_{l_1}, t_1 + (i_{l_2} - 1) \cdot T_s + \tau_{l_1} + \tau_{l_2}], N_2 \geq i_{l_2} \geq 1.$$

Здесь τ_{l_2} – длительность временного интервала, соответствующего 2-му участку ВОЛС длиной l_2 . Момент t_1 определяется одной из формул (3.24) – (3.25), если за предельное число временных кадров не зарегистрирован фотон, или формулой (3.28) при отрицательном результате тестирования.

Для предельного числа временных кадров, допустимых для анализа 2-го участка ВОЛС N_2 , всегда выполняется условие $N_1 < N_2$.

Если за предельное число временных кадров N_2 не зарегистрирован фотон, то аппаратура переходит к проверке третьего участка ВОЛС протяжённостью l_3 . В этом случае момент окончания поиска в 2-м участке ВОЛС

$$t_{l_2} = t_1 + \tau_{l_2} + (N_2 - 1) \cdot T_s. \quad (3.29)$$

Если переход к анализу нового участка ВОЛС жёстко привязан к тактовым импульсам генератора в блоке управления, то момент окончания поиска в 2-м участке ВОЛС составит

$$t_{l_2} = t_1 + N_2 \cdot T_s. \quad (3.30)$$

При регистрации фотона в момент $t_{l_2s_1}$ в i_{l_2} -м кадре при анализе 2-го участка ВОЛС аппаратура переходит к тестированию, при котором повторный опрос фотодетектора производится последовательно в интервалах

$$[t_{l_2strob_1} + (k_2 - 1) \cdot T_s, t_{l_2strob_2} + (k_2 - 1) \cdot T_s], k_2 = \overline{1, N_{test.2}}.$$

Здесь

$$t_{l_2strob_1} = t_{l_2s_1} + \Delta\tau + T_s - 0,5 \cdot \tau_{strob},$$

$$t_{l_2strob_2} = t_{l_2s_1} + \Delta\tau + T_s + 0,5 \cdot \tau_{strob}.$$

Для моделирования момента приёма фотона $t_{l_2s_1}$ в i_{l_2} -м кадре при анализе 2-го участка ВОЛС можно использовать формулу

$$t_{l_2s_1} = t_1 + RNG_{l_2s_1} \cdot \tau_{l_2} + (i_{l_2} - 1) \cdot T_s.$$

Момент обнаружения фотонного импульса в i_{l_2} -м кадре при k_2 -м тесте 2-го участка ВОЛС определяется формулой

$$t_{l_2D} = t_{l_2s_2} = t_{l_2strob_1} + RNG_{l_2s_2} \cdot \tau_{strob} + (k_2 - 1) \cdot T_s.$$

или

$$t_{l_2D} = t_1 + (i_{l_2} + k_2 - 1) \cdot T_s + \Delta\tau - 0,5 \cdot \tau_{strob} + RNG_{l_2s_2} \tau_{strob} + RNG_{l_2s_1} \tau_{l_2}. \quad (3.31)$$

Если же за предельное допустимое количество тестов $N_{test.2}$ приём фотона не зафиксирован, то аппаратура вновь возвращается в режим поиска. Момент отрицательного результата тестирования в i_{l_2} -м кадре при последнем $N_{test.2}$ -м тесте 2-го участка ВОЛС может быть определён по формуле

$$t_{l_2ND} = t_{l_2strob_1} + (N_{test.2} - 1) \cdot T_s + \tau_{strob}$$

или

$$t_{l_2ND} = t_1 + (i_{l_2} + N_{test.2} - 1)T_s + \Delta\tau + 0,5\tau_{strob} + RNG_{l_2s_1} \tau_{l_2} \quad (3.32)$$

Если за предельное допустимое количество кадров N_2 на этапе поиска или тестов $N_{test.2}$ на этапе тестирования приём фотона не зафиксирован, то теперь проверяется уже третий участок ВОЛС с протяжённостью l_3 .

Условные временные параметры при анализе j -го участка ВОЛС. Из анализа формул (3.24) – (3.32) методом математической индукции следуют формулы для определения:

- момента обнаружения фотонного синхроимпульса в i_{l_j} -м кадре ($N_j \geq i_{l_j} \geq 1$) j -го участка ВОЛС ($j = \overline{1, N_{FOL}}$) длиной l_j при проведении k_j -го ($N_{test.j} \geq k_j \geq 1$) тестирования

$$t_{l_jD} = t_{(j-1)} + (i_{l_j} + k_j - 1) \cdot T_s + \Delta\tau - 0,5 \cdot \tau_{strob} + RNG_{l_js_1} \tau_{l_j} + RNG_{l_js_2} \tau_{strob}; \quad (3.33)$$

– момента отрицательного результата тестирования в i_{l_j} -м кадре ($N_j \geq i_{l_j} \geq 1$) при последнем $N_{test,j}$ -м тесте j -го участка ВОЛС

$$t_{l_j ND} = t_{(j-1)} + (i_{l_j} + N_{test,j} - 1) \cdot T_s + \Delta\tau + 0,5 \cdot \tau_{strob} + RNG_{l_{js1}} \cdot \tau_{l_j}; \quad (3.34)$$

– времени на анализ j -го ($j = \overline{1, N_{FOL}}$) участка ВОЛС, где за предельное число временных кадров N_j не был зарегистрирован фотон,

$$t_{l_j} = t_{(j-1)} + \tau_{l_j} + (N_j - 1) \cdot T_s, \quad (3.35)$$

где $t_{l_0} = 0$.

Если за предельное число временных кадров N_j при анализе j -го участка ВОЛС не зарегистрирован фотон, то аппаратура переходит к проверке $(j+1)$ -го участка протяжённостью l_{j+1} . Если при проверке всех участков не зафиксирован приём фотона, то аппаратура возвращается к обследованию первого участка ВОЛС.

В формулах (3.33) – (3.35) время анализа временного интервала t_j , соответствующего j -му участку ВОЛС длиной l_j , определяется формулой (3.34) при отрицательном результате тестирования или формулой (3.35) при отсутствии регистрации фотонного импульса за предельное число временных кадров.

Энергетические характеристики. Пусть фотон регистрируется в момент $t_{l_{js1}}$, соответствующий j -му участку при разнесении корреспондентов на

$$L_s = v_{OF} \cdot \left(\sum_{z=1}^{j-1} \tau_{l_z} + RNG_{l_{js1}} \cdot \tau_{l_j} \right).$$

Отметим, что коэффициент ослабления фотонного импульса при анализе j -го участка ВОЛС ($j = \overline{1, N_{FOL}}$) в децибелах будет определяться формулой

$$K_{s,j}[\text{дБ}] = \alpha_{OF} \left[\frac{\text{дБ}}{\text{км}} \right] \cdot v_{OF} \left[\frac{\text{км}}{\text{с}} \right] \cdot \left(\sum_{z=1}^{j-1} \tau_{l_z}[\text{с}] + RNG_{l_{js1}} \cdot \tau_{l_j}[\text{с}] \right), \quad (3.36)$$

где α_{OF} – погонное затухание излучения в применяемом оптическом волокне.

Среднее число регистрируемых фотонов за длительность фотонного импульса при анализе j -го участка ВОЛС равно

$$\overline{n_{s,j}} = \overline{n_{s,0}} \cdot 10^{-\frac{K_{s,j}[\text{дБ}]}{10}}. \quad (3.37)$$

На практике всегда среднее число $\overline{n_{s,j}}$ значительно превышает среднее число ИТТ и послеимпульсов $\overline{n_{DCR,s}} = \xi_{DCR} \cdot \tau_s$ за длительность импульса стробирования. При этом среднее число регистрируемых фотонов и ИТТ за время стробирования при анализе j -го участка ВОЛС определяется формулой (3.8).

Отметим, что статистические свойства потока фотонов и ИТТ описываются законом Пуассона $Pr\{n|\bar{n}\}$, где вероятность генерации n событий определяется средним числом фотонов и/или ИТТ $\bar{n}$ за время наблюдения (длительность временного кадра, оптического импульса или импульса стробирования).

Резюме. Получены аналитические выражения для расчета временных характеристик предлагаемого алгоритма синхронизации. При отрицательном результате поиска фотонного импульса во всех участках, аппаратура возвращается к обследованию 1-го участка ВОЛС. При успешном тестирования этап «грубой» оценки момента приема фотонного импульса считается завершённым. Получены аналитические выражения для расчета энергетических характеристик алгоритма синхронизации. Статистические свойства потока фотонов и ИТТ описываются законом Пуассона.

3.5 Методика расчёта условных вероятностных характеристик двухэтапного временного алгоритма синхронизации

Рассмотрим ситуацию, при которой, приступая к синхронизации приёмопередающей и кодирующей станций, отсутствует априорная информация о расстоянии между станциями. Следовательно, имеется информация только о том, что протяжённость ВОЛС не может превышать значения L_{FOL} . Причём $L_{FOL} \leq L_{lim}$, где значение L_{lim} определяется формулой (3.20).

При разделении ВОЛС с общей протяжённостью L_{FOL} на N_{FOL} участков с убывающими длинами, рассчитываемыми по формуле (3.19), вероятность нахождения фотонного импульса в j_s -м участке длиной l_{j_s} равна

$$p(l_{j_s}) = l_{j_s}/L_{FOL}, j_s = \overline{1, N_{FOL}}. \quad (3.38)$$

Условная вероятность отсутствия приёма фотона и/или ИТТ за время анализа j -го участка ВОЛС τ_{lj} равна

$$P_{DCR0.j} = \begin{cases} \exp(-\overline{n_{DCR.j}}), & j = \overline{1, J_s - 1} \text{ и } j = \overline{J_s + 1, N_{FOL}}; \\ \exp(-\overline{n_{s.j}} - \overline{n_{DCR.j}}), & j = j_s. \end{cases} \quad (3.39)$$

Расчёт условной вероятности регистрации хотя бы одного фотона или ИТТ при анализе j -го участка проводится по формулам

$$P_{Ds.j} = \begin{cases} 1 - \exp(-\overline{n_{DCR.j}}) = 1 - P_{DCR0.j}, & j \neq j_s; \\ 1 - \exp(-\overline{n_{s.j}} - \overline{n_{DCR.j}}), & j = j_s. \end{cases} \quad (3.40)$$

Условная вероятность отсутствия регистрации фотона и/или ИТТ за предельное число временных кадров N_j в j -м участке ВОЛС равна

$$P_{D.j}\{N_j\} = \begin{cases} 1 - \frac{1 - \exp(-\overline{n_{DCR.j}})}{\overline{n_{DCR.j}}} \cdot (1 - P_{DCR0.j}^{N_j}), & j \neq j_s; \\ 1 - \frac{1 - \exp(-\overline{n_{DCR.j}})}{\overline{n_{DCR.j}}} \cdot \frac{1 - P_{DCR0.j}^{N_j}}{1 - P_{DCR0.j}} \cdot P_{Ds.j}, & j = j_s. \end{cases} \quad (3.41)$$

Резюме. Получены аналитические формулы для расчёта условных временных параметров при отсутствии априорной информации о расстоянии между станциями в случае, если анализируемый участок является сигнальным, и в обратном случае, если участок является шумовым.

3.6 Анализ временных характеристик на этапе тестирования в сигнальном участке ВОЛС

Пусть на этапе поиска фотон регистрируется в момент $t_{lj_{s1}}$ в i_{lj} -м кадре ($N_j \geq i_{lj} \geq 1$) во время анализа j -го участка ВОЛС, причём j -й участок является сигнальным. Если на этапе тестирования повторное обнаружение фотонного импульса произошло в момент t_{ljD} (см. формулу (3.33)) при k_j -м тесте ($N_{test.j} \geq k_j \geq 1$), то время тестирования составит

$$\tau_{test.k_j} = t_{ljD} - t_{lj_{s1}} = k_j \cdot T_s - 0,5 \cdot \tau_{strob} + RNG_{lj_{s2}} \cdot \tau_{strob}.$$

Тогда среднее время тестирования, завершающегося обнаружением фотонного импульса, может быть рассчитано по формуле

$$\begin{aligned}
\overline{\tau_{test.D.j}} &= \int_0^1 dRNG_{l_j s_2} \cdot \left[\sum_{k_j=1}^{N_{test.j}} p(k_j) \cdot \tau_{test.k_j} \right] = T_s \cdot \left[\sum_{k_j=1}^{N_{test.j}} k_j \cdot p(k_j) \right]. \\
\overline{\tau_{test.D.j}} &= \int_0^1 dRNG_{l_j s_2} \cdot \left[\sum_{k_j=1}^{N_{test.j}} p(k_j) \cdot \tau_{test.k_j} \right] \\
&= \left[\sum_{k_j=1}^{N_{test.j}} p(k_j) \cdot k_j \cdot T_s \right] - \frac{\tau_{strob}}{2} + \left[\int_0^1 RNG_{l_j s_2} \cdot \tau_{strob} \cdot dRNG_{l_j s_2} \right] \\
&= T_s \cdot \left[\sum_{k_j=1}^{N_{test.j}} k_j \cdot p(k_j) \right] - \frac{\tau_{strob}}{2} + \frac{\tau_{strob}}{2} = T_s \cdot \left[\sum_{k_j=1}^{N_{test.j}} k_j \cdot p(k_j) \right].
\end{aligned}$$

Учитывая, что число фотонов и ИТТ за время стробирования подчинено закону Пуассона, находим условную вероятность обнаружения фотонного импульса при проведении k_j -го тестирования при анализе j -го участка ВОЛС

$$p(k_j) = [1 - \exp(-\overline{n_{strob.j}})] \cdot \exp[-(k_j - 1) \cdot \overline{n_{strob.j}}].$$

Среднее время тестирования $\overline{\tau_{test.D.j}}$, завершающегося обнаружением во время анализа j -го участка, может быть рассчитано по формуле

$$\begin{aligned}
\overline{\tau_{test.D.j}} &= [1 - \exp(-\overline{n_{strob.j}})] \cdot T_s \\
&\cdot \left[\sum_{k_j=1}^{N_{test.j}} k_j \cdot \exp[-(k_j - 1) \cdot \overline{n_{strob.j}}] \right]. \tag{3.42}
\end{aligned}$$

Результаты расчётов по (3.42) для сигнального участка сведены в таблицу 3.8.

Таблица 3.8 – Среднее время тестирования в сигнальном участке, завершающегося обнаружением фотонного импульса (в мс)

$P_{err.0}$	Номер участка									
	1	2	3	4	5	6	7	8	9	10
0,01	1,10	1,34	1,58	1,83	2,08	2,33	2,58	2,83	3,08	3,34
0,02	2,59	3,50	4,43	5,39	6,36	7,34	8,33	9,33	10,34	11,35
0,05	10,63	16,93	23,63	30,59	37,74	44,96	52,31	59,72	67,22	74,71
0,10	29,1	52,9	70,0	106,4	134,7	163,6	192,8	222,5	252,4	282,5

На рисунке 3.7 представлена зависимость среднего времени тестирования, завершающегося обнаружением фотонного импульса, от номера участка, в котором обнаружен фотонный импульс (при допущении отсутствия временных отклонений

моментов прихода фотона вследствие наличия в оптическом волокне хроматической и поляризационной дисперсий).

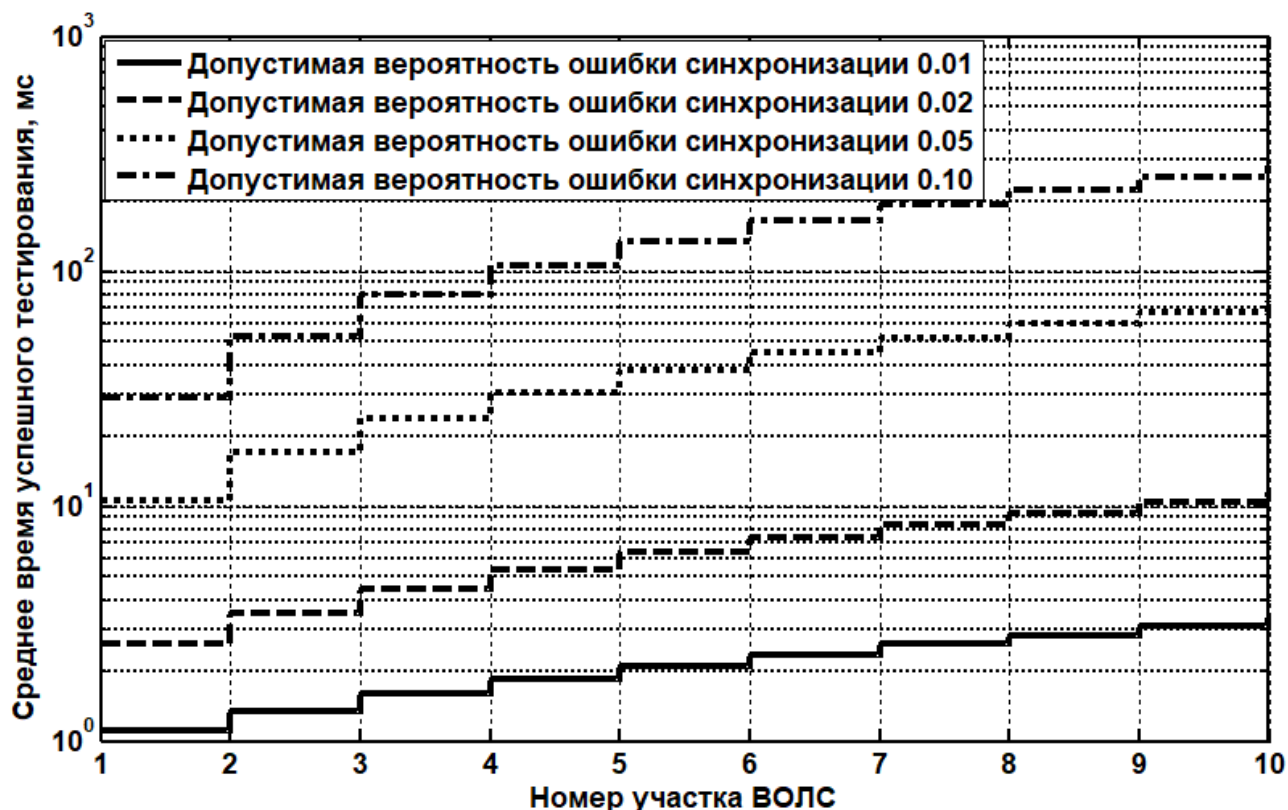


Рисунок 3.7 – Среднее время тестирования, завершающегося обнаружением фотонного импульса, при анализе сигнального j -го участка ВОЛС

Увеличение среднего времени тестирования от участка к участку обусловлено значительным увеличением рекомендуемого количества тестов с ростом номера участка ВОЛС. Так, если различие в количестве тестов при $P_{err.0}=0,10$ между 1-м и 2-м участками составляет 1,8 раза, то при сравнении 1-го и 10-го участков различие достигает уже 9,8 раза. При этом среднее время тестирования при анализе 10-го участка ВОЛС составляет 282,54 мс, что в 9,7 раза больше среднего времени тестирования в 1-м участке (29,13 мс).

Среднее число тестов для сигнальных участков ВОЛС для ряда вероятностей ошибок синхронизации сведены в таблицу 3.9. Здесь же приведено предельно-допустимое число тестов. Отношение среднего к предельному числу тестов практически постоянно во всех участках ВОЛС (отклонение не более 3 % при $P_{err.0}=0,01$ и 1,5 % при $P_{err.0}=0,10$). С уменьшением допустимой вероятности ошибки синхронизации с 0,1 до 0,01 указанное отношение падает с 6,90 до 4,87.

Отметим, период следования оптических импульсов равен $T_s=83,33; 166,67; 500$ и 1000 мкс при $P_{err.0} = 0,01; 0,02; 0,05$ и $0,10$ соответственно.

Таблица 3.9 – Среднее число затрачиваемых тестов при положительном результате тестирования в сигнальном участке/предельное число тестов

$P_{err.0}$	Номер участка									
	1	2	3	4	5	6	7	8	9	10
0,01	$\frac{13,23}{89}$	$\frac{16,10}{109}$	$\frac{19,01}{129}$	$\frac{21,95}{150}$	$\frac{24,93}{171}$	$\frac{27,92}{191}$	$\frac{30,92}{212}$	$\frac{33,94}{233}$	$\frac{36,96}{254}$	$\frac{40,02}{276}$
0,02	$\frac{15,53}{95}$	$\frac{20,98}{130}$	$\frac{26,59}{165}$	$\frac{32,33}{201}$	$\frac{38,19}{238}$	$\frac{44,06}{275}$	$\frac{49,97}{312}$	$\frac{55,99}{350}$	$\frac{62,03}{388}$	$\frac{68,07}{427}$
0,05	$\frac{21,26}{114}$	$\frac{33,85}{183}$	$\frac{47,26}{256}$	$\frac{61,18}{332}$	$\frac{75,48}{411}$	$\frac{89,93}{490}$	$\frac{104,62}{570}$	$\frac{119,45}{651}$	$\frac{134,45}{733}$	$\frac{149,43}{815}$
0,10	$\frac{29,13}{140}$	$\frac{52,89}{256}$	$\frac{78,99}{383}$	$\frac{106,41}{517}$	$\frac{134,73}{655}$	$\frac{163,56}{796}$	$\frac{192,81}{939}$	$\frac{222,46}{1083}$	$\frac{252,36}{1229}$	$\frac{282,54}{1376}$

С высокой точностью $p_{test0} = 1 - \overline{n_{DCR.strob}}$, $1 - p_{test0} = \overline{n_{DCR.strob}}$. Тогда

$$\overline{\tau_{test.D.j}} = T_s \cdot \overline{n_{DCR.strob}} \cdot \left[\sum_{k_j=1}^{N_{test.j}} k_j \cdot (1 - \overline{n_{DCR.strob}})^{k_j-1} \right].$$

Поскольку $\overline{n_{DCR.strob}} \ll 1$, то, используя бином Ньютона, находим

$$(1 - \overline{n_{DCR.strob}})^{k_j-1} = 1 - (k_j - 1) \cdot \overline{n_{DCR.strob}}.$$

Откуда

$$\begin{aligned} \overline{\tau_{test.D.j}} &= T_s \cdot \overline{n_{DCR.strob}} \cdot (1 + \overline{n_{DCR.strob}}) \cdot \frac{N_{test.j} \cdot (N_{test.j} + 1)}{2} - \\ &\rightarrow -T_s \cdot \overline{n_{DCR.strob}}^2 \cdot \frac{N_{test.j} \cdot (N_{test.j} + 1) \cdot (2 \cdot N_{test.j} + 1)}{6}. \end{aligned}$$

Справедливо приближение

$$\overline{\tau_{test.D.j}} = T_s \cdot \overline{n_{DCR.strob}} \cdot \frac{N_{test.j}^2}{2} - T_s \cdot \overline{n_{DCR.strob}}^2 \cdot \frac{N_{test.j}^3}{3}.$$

Безусловное среднее время тестирования участка ВОЛС может быть рассчитано по формуле

$$\overline{\tau_{test.j}} = Pr_{test.0.j} \cdot \overline{\tau_{test.0.j}} + Pr_{test.D.j} \cdot \overline{\tau_{test.D.j}},$$

где $Pr_{test.D.j}$ – вероятность повторного срабатывания на этапе тестирования в j -м сигнальном участке, $Pr_{test.0.j}$ – вероятность повторного ложного срабатывания на

этапе тестирования в j -м шумовом участке, $\overline{\tau_{test.0.j}}$ – среднее время тестирования шумового участка, завершающегося повторным ложным срабатыванием.

Причём вероятность повторного срабатывания на этапе тестирования в j -м сигнальном участке ВОЛС составляет

$$Pr_{test.D.j} = \sum_{k_j=1}^{N_{test.j}} p_{test}^{k_j-1} \cdot (1 - p_{test}) = (1 - p_{test}) \cdot \sum_{k_j=1}^{N_{test.j}} p_{test}^{k_j-1},$$

где $p_{test} = \exp(-\overline{n_{strob.j}})$ – вероятность отсутствия регистрации события (повторного приема фотона) во время теста.

Резюме. Проведен анализ временных характеристик этапа тестирования в сигнальном участке ВОЛС. Среднее время тестирования увеличивается от участка к участку, что обусловлено значительным увеличением рекомендуемого количества тестов с ростом номера участка ВОЛС.

3.7 Методика расчёта времени тестирования при ложном решении на этапе поиска

Проанализируем случай принятия ложного решения на этапе поиска в j -м участке. Тогда на этапе тестирования за время стробирования будет регистрироваться в среднем $\overline{n_{DCR.strob}} = \xi_{DCR} \cdot \tau_{strob}$ ИТТ. Причём вероятность отсутствия регистрации события (повторного приёма ИТТ) во время теста равна $p_{test0} = \exp(-\overline{n_{DCR.strob}})$.

Обнаружение ложного срабатывания на этапе поиска происходит с вероятностью $Pr_{test.D0.j} = p_{test0}^{N_{test.j}} = \exp(-N_{test.j} \cdot \overline{n_{DCR.strob}})$. Причём время тестирования равно $\tau_{test.D0.j} = N_{test.j} \cdot T_s$.

Пусть, как и ранее, на этапе поиска импульс темнового тока регистрируется в момент t_{ljs_1} в i_{lj} -м кадре ($N_j \geq i_{lj} \geq 1$) во время анализа j -го шумового участка ВОЛС. Если на этапе тестирования повторный приём ИТТ произошёл в момент t_{ljD} при k_j -м тесте ($N_{test.j} \geq k_j \geq 1$), то время тестирования составит

$$\tau_{test.k_j} = t_{ljD} - t_{ljs_1} = k_j \cdot T_s - 0,5 \cdot \tau_{strob} + RNG_{ljs_2} \cdot \tau_{strob}.$$

Причём вероятность повторного ложного срабатывания на этапе тестирования в j -м шумовом участке ВОЛС составляет (рисунок 3.8)

$$Pr_{test.0,j} = \sum_{k_j=1}^{N_{test,j}} p_{test0}^{k_j-1} \cdot (1 - p_{test0}) = (1 - p_{test0}) \cdot \sum_{k_j=1}^{N_{test,j}} p_{test0}^{k_j-1}$$

$$= (1 - p_{test0}) \cdot \sum_{k_j=1}^{N_{test,j}} \exp(-(k_j - 1) \cdot \overline{n_{DCR.strob}}).$$

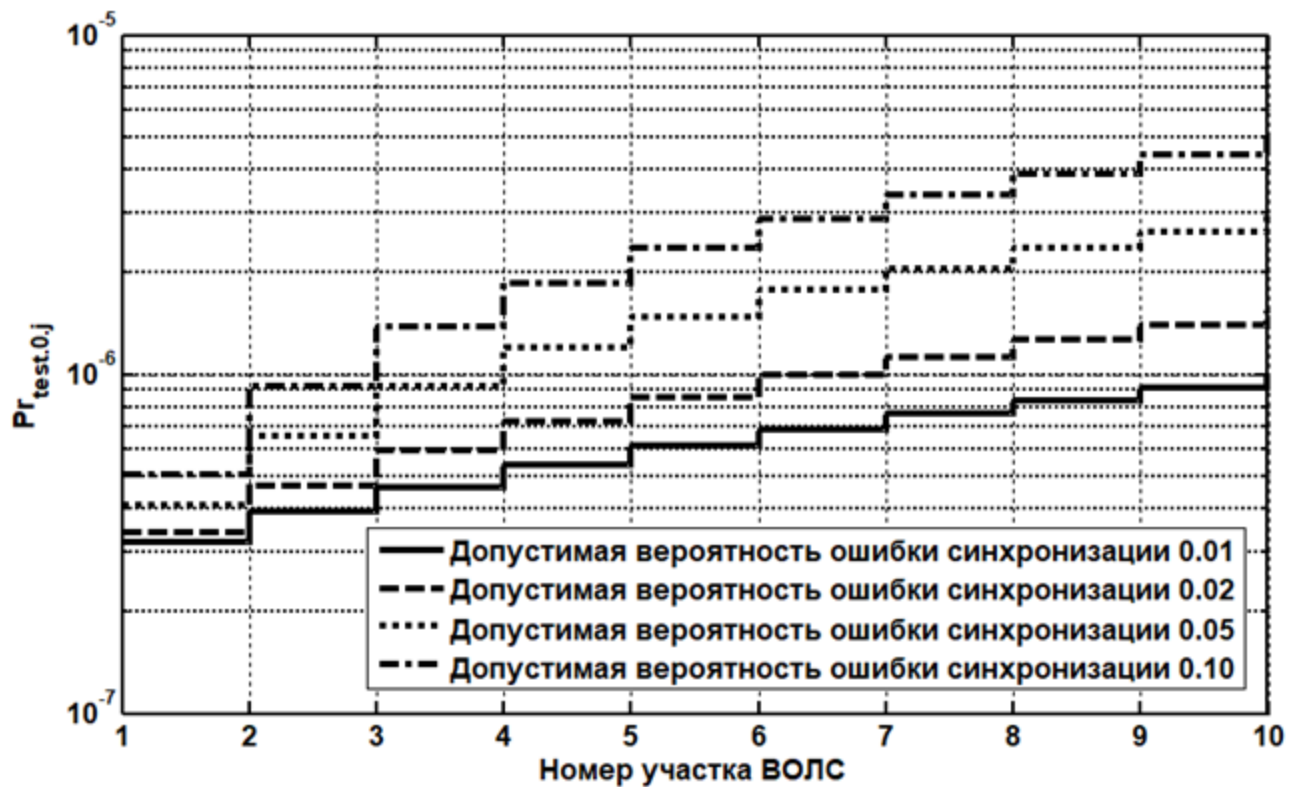


Рисунок 3.8 – Вероятность повторного ложного срабатывания на этапе тестирования в шумовом участке ВОЛС

Тогда среднее время тестирования шумового участка, завершающегося повторным ложным срабатыванием, может быть рассчитано по формуле

$$\overline{\tau_{test.0,j}} = \int_0^1 dRNG_{l_j s_2} \cdot \left[\sum_{k_j=1}^{N_{test,j}} \tau_{test.k_j} \cdot p_{test0}^{k_j-1} \cdot (1 - p_{test0}) \right].$$

Произведя интегрирование, находим среднее время тестирования в шумовом участке

$$\overline{\tau_{test.0,j}} = T_s \cdot (1 - p_{test0}) \cdot \left[\sum_{k_j=1}^{N_{test,j}} k_j \cdot p_{test0}^{k_j-1} \right].$$

Воспользовавшись (4.1.7.2) в [110], находим формулу для расчёта среднего числа тестов в шумовом участке

$$\overline{N_{test.0,j}} = \frac{1}{1 - p_{test0}} [1 - (N_{test,j} + 1 - N_{test,j} p_{test0}) p_{test0}^{N_{test,j}}]. \quad (3.43)$$

Результаты расчётов по (3.43) для j-го шумового участка ВОЛС сведены в таблицу 3.10. Видно, что вследствие достаточно низкой вероятности повторного ложного срабатывания на этапе тестирования в шумовом участке ВОЛС увеличением результирующего среднего времени тестирования можно пренебречь.

Таблица 3.10 – Среднее число тестов в шумовом участке, делённое на 100000

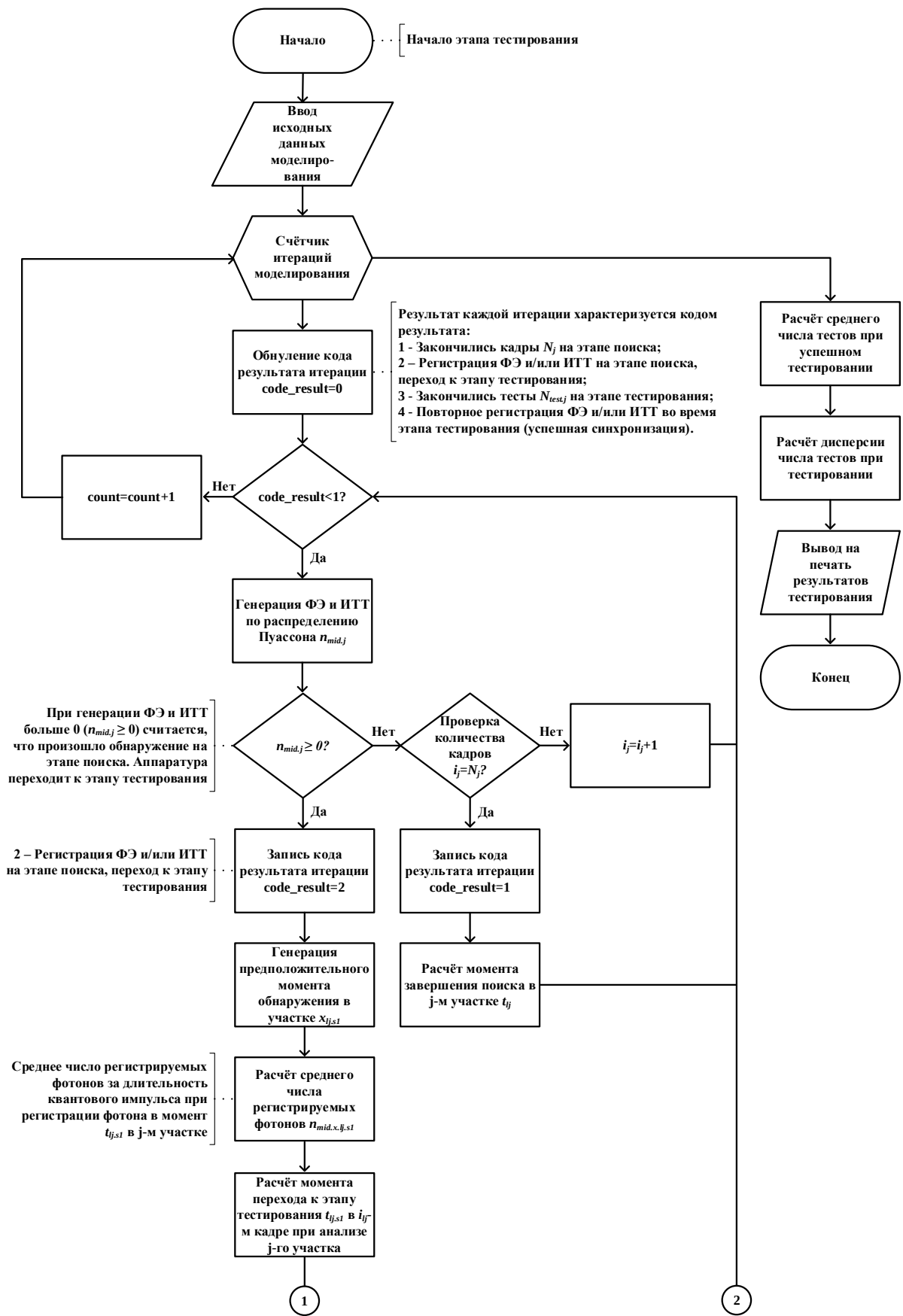
$P_{err.0}$	Номер участка									
	1	2	3	4	5	6	7	8	9	10
0,01	1,6	2,1	3,2	3,9	5,5	6,6	7,7	9,8	11	14
0,02	1,8 ⁵	3,0	4,8	7,6	10	14	18	22	28	33
0,05	2,5	6,1	12	19	31	43	58	78	97	120
0,10	3,8	12	26	49	78	110	160	210	270	340

Резюме. Полученные аналитические формулы для расчёта энергетических, временных и вероятностных характеристик позволяют перейти к моделированию процесса синхронизации.

3.8 Моделирование этапа тестирования при нахождении однофотонного источника излучения в сигнальном участке ВОЛС

Посредством моделирования этапа тестирования определим среднее и дисперсию числа тестов ($N_{test,j} \geq k_j \geq 1$), затрачиваемых при анализе 1-го участка ВОЛС. Примем, что 1-й участок является сигнальным.

Блок-схема алгоритма тестирования 1-го участка представлена на рисунке 3.9. Этап тестирования заключается в повторном опросе фотодетектора только в интервалах ожидаемого прихода фотонного импульса во время стробирования за допустимое количество тестов для данного участка $N_{test.1}$. При успешном тестировании (при повторной регистрации фотонов или ИТТ) аппаратура переходит к этапу точной оценки момента приёма синхроимпульса. Если за предельное число тестов для данного участка $N_{test.1}$ повторной регистрации фотонов и/или ИТТ не обнаружено, аппаратура переходит в режим поиска для анализа следующего участка.



a)

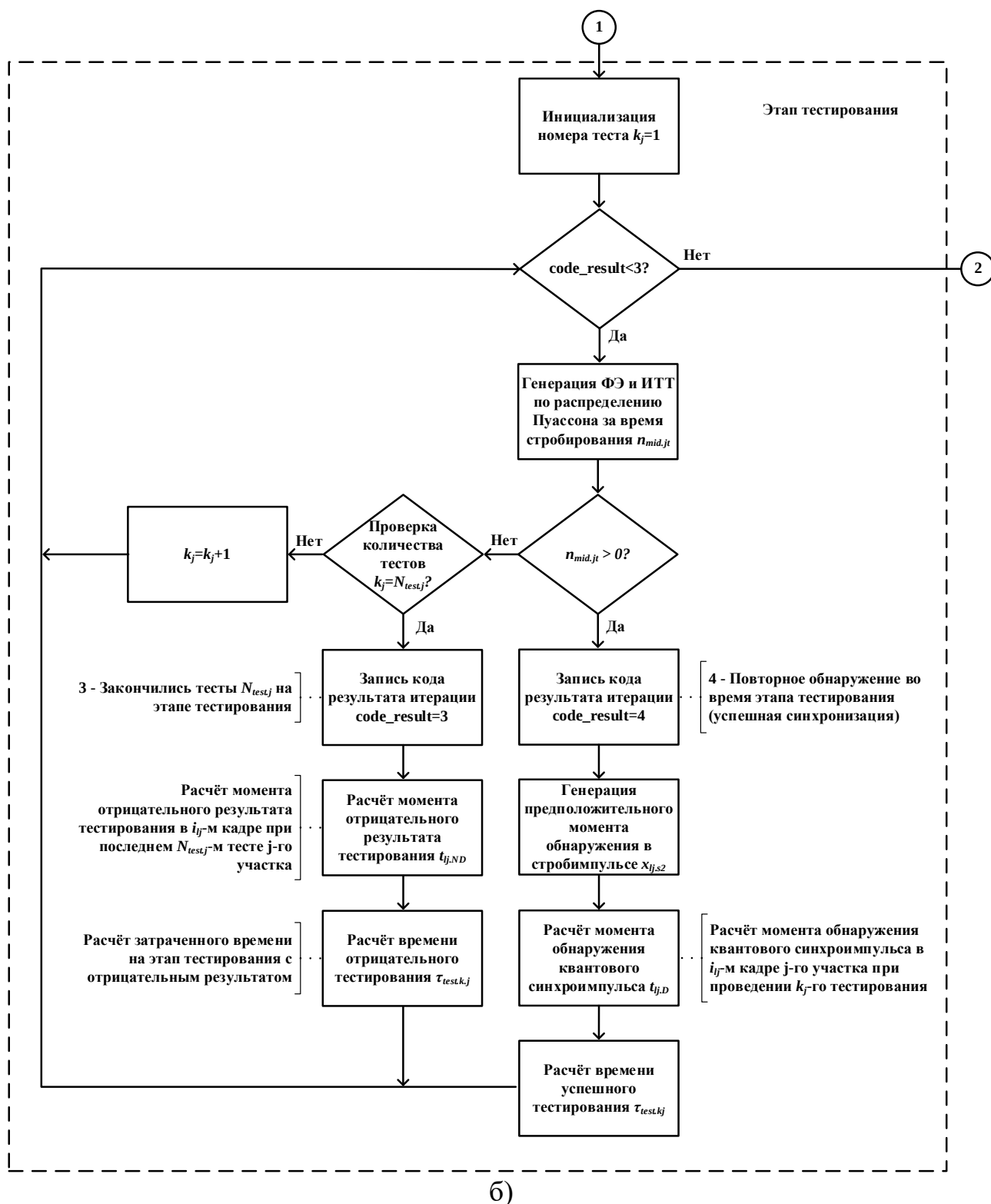


Рисунок 3.9 – Блок-схема алгоритма тестирования 1-го участка ВОЛС

Частота генерации ИТТ принята равной $\xi_{DCR}=6$ Гц [107], что соответствует применению ОЛФД id210-SFM-C при квантовой эффективности фотокатода 10 %. Среднее число фотонов за длительность оптического импульса на выходе из кодирующей станции – $\overline{n_{s0}}=0,1$. Допустимая вероятность ошибки синхронизации

$P_{err.0}=0,01; 0,02; 0,05; 0,10$. Период следования оптических импульсов равен $T_s=83,33; 166,67; 500$ и 1000 мкс при $P_{err.0}= 0,01; 0,02; 0,05$ и $0,10$ соответственно.

В таблицу 3.11 сведены результаты моделирования перехода к этапу тестирования в 1-м участке при условии, что участок является сигнальным.

Таблица 3.11 – Результаты моделирования перехода к этапу тестирования в сигнальном (первом) участке ВОЛС, количество экспериментов 100000

Параметры этапа тестирования		$P_{err.0}$			
		0,01	0,02	0,05	0,10
Среднее число тестов при успешном тестировании. Модель/теория (табл. 3.9)		13,23	15,49	21,46	29,40
Среднее время успешного тестирования, мс. Модель/теория (табл. 3.8)		1,1	2,58	10,73	29,40
Вероятность успешной синхронизации. Модель/теория (ф. 3.1)		0,995	0,989	0,972	0,944
Вероятность отсутствия регистрации ФЭ и/или ИТТ в сигнальном участке. Модель/теория (ф. 3.41)		0,004	0,009	0,023	0,046
		0,009	0,018	0,045	0,089
Этап тестирования	Вероятность успешного тестирования. Модель/теория	0,99895	0,99793	0,99470	0,99003
		0,99903	0,99807	0,99520	0,99024
	Вероятность ошибки тестирования. Модель/теория (ф. 3.3)	0,00105	0,00207	0,00530	0,00997
		0,00097	0,00193	0,00480	0,00976
Время тестирования с отрицательным результатом, мс. Модель		7,42	15,83	57,00	140,00

При моделировании исключается нестабильность периода следования синхроимпульсов $\Delta T_s = 0$. Принято, что отсутствует временная задержка между моментами приёма и регистрации фотона Δt . В качестве среды распространения принято оптическое волокно, где отсутствуют хроматическая и поляризационная дисперсии Δt_{FOL} .

При анализе 1-го участка возможны следующие результаты: отсутствие регистрации фотона и/или ИТТ (события) на этапе поиска, успешная синхронизация, отсутствие повторной регистрации события на этапе тестирования (отрицательный результат). Суммарная вероятность данных событий равна 1. Анализируя результаты моделирования, при $P_{err.0}=0,05$ вероятность отсутствия регистрации события на этапе поиска равна 0,023, соответственно переход к этапу

тестирования осуществлен в 97691 эксперименте из 100000. Вероятность успешной синхронизации равна 0,972, следовательно, вероятность отсутствия синхронизации в 1-м участке вследствие отрицательного результата тестирования равна 0,005. На этапе тестирования распределение вероятностей успешное/отрицательное тестирование составляет 0,995/0,005.

Среднее число тестов за все итерации при различных допустимых вероятностях ошибки синхронизации не превышает 21% от предельного числа тестов для данного участка ($N_{test.1}=89; 95; 114$ и 140 при $P_{err.0}=0,01; 0,02; 0,05$ и $0,10$ соответственно). Причем отклонение полученных результатов в ходе моделирования от теоретически рассчитанных не превышает $\pm 1\%$. Вероятность ошибки тестирования значительно увеличивается при ухудшении требований к допустимой вероятности ошибки синхронизации (в 10 раз при $P_{err.0}=0,10$ и $P_{err.0}=0,01$). Среднее время успешного тестирования увеличивается более чем в 26 раз при ухудшении допустимой вероятности ошибки синхронизации с $P_{err.0}=0,01$ до $P_{err.0}=0,10$. Время отрицательного тестирования при отсутствии повторной регистрации фотона за предельное число тестов также увеличивается более чем в 18 раз при увеличении допустимой вероятности ошибки с $P_{err.0}=0,01$ до $P_{err.0}=0,10$.

Различие вероятностей успешного тестирования при моделировании и теоретических расчётах не превышает 0,05% при различных значениях допустимой вероятности ошибки синхронизации. Различие вероятностей ошибки тестирования при моделировании и теоретических расчётах не превышает 10,5%.

Резюме. Посредством моделирования этапа тестирования определены среднее число тестов и среднее время при успешном тестировании, вероятностные характеристики этапа тестирования в 1-м участке ВОЛС. Проведен сравнительный анализ полученных при моделировании результатов с результатами теоретических исследований. Различие вероятностей успешного тестирования и ошибки тестирования при моделировании и теоретических расчётах не превышает 0,05 и 10,5% соответственно, что подтверждает возможность использовать полученные аналитические выражения.

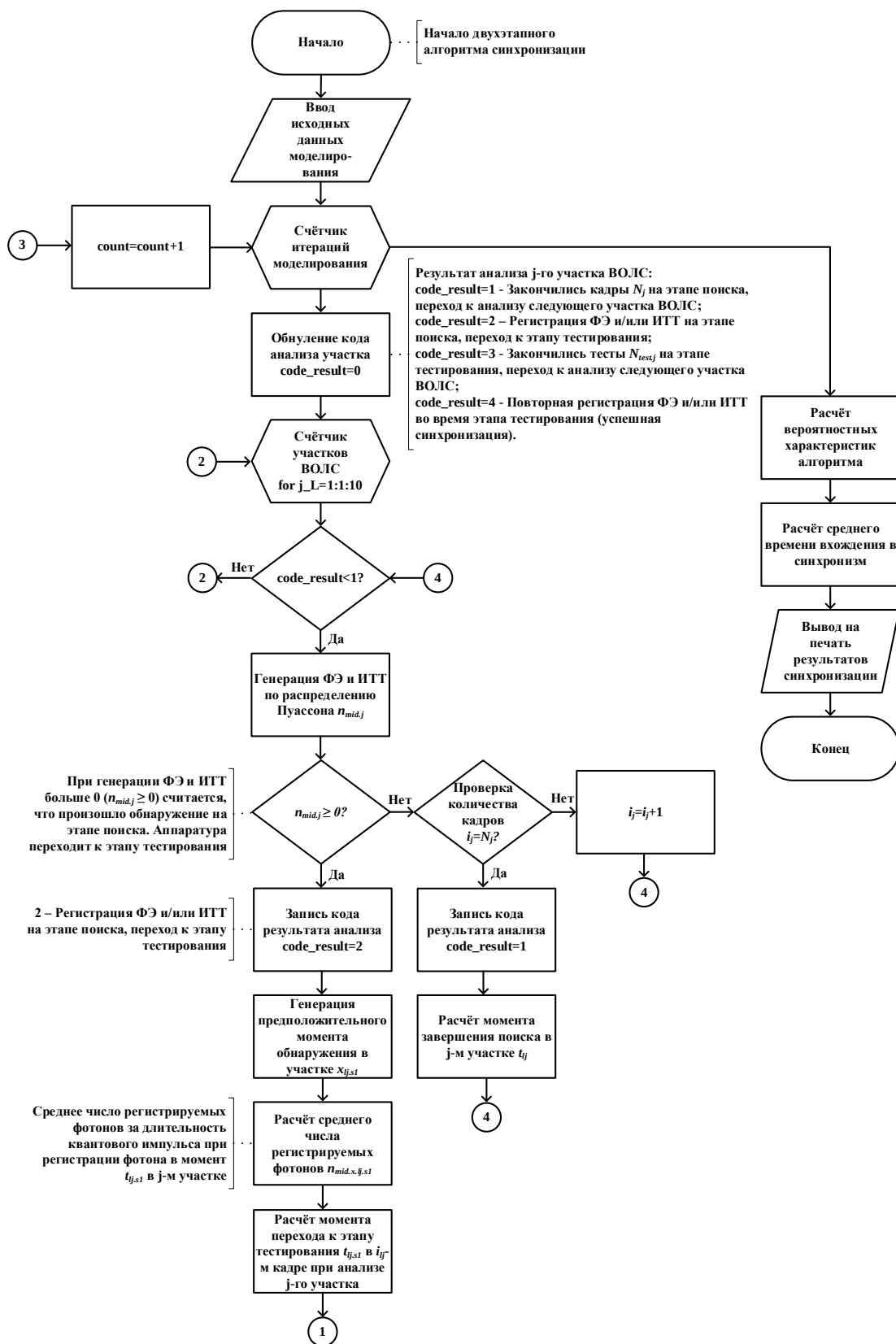
3.9 Моделирование двухэтапного алгоритма синхронизации станций с разбиением волоконно-оптической линии на участки с убывающей длиной

Посредством моделирования определим временные и вероятностные характеристики предлагаемого двухэтапного алгоритма синхронизации при нахождении однофотонного источника излучения в j -м участке ВОЛС.

Блок-схема двухэтапного алгоритма синхронизации представлена на рисунке 3.10. Анализ j -го участка на наличие однофотонного источника излучения завершается с одним из следующих результатов: закончились кадры N_j на этапе поиска, переход к анализу следующего участка; регистрация события на этапе поиска, переход к этапу тестирования; закончились тесты $N_{test,j}$ на этапе тестирования, переход к анализу следующего участка ВОЛС; повторная регистрация события во время этапа тестирования (успешная синхронизация).

При моделировании исключается нестабильность периода следования синхроимпульсов $\Delta T_s = 0$. Принято, что отсутствует временная задержка между моментами приёма и регистрации фотона $\Delta \tau$. В качестве среды распространения принято ОВ, где отсутствуют хроматическая и поляризационная дисперсии $\Delta \tau_{FOL}$.

Частота генерации ИТТ принята равной $\xi_{DCR}=6$ Гц [107], что соответствует применению однофотонного лавинного фотодиода (ЛФД) id210-SFM-C (Standard) при квантовой эффективности фотокатода 10 %. Среднее число фотонов за длительность оптического импульса на выходе из кодирующей станции – $\overline{n_{s0}}=0,1$. Допустимая вероятность ошибки синхронизации $P_{err,0}=0,01; 0,02; 0,05; 0,10$. Период следования оптических импульсов равен $T_s=83,33; 166,67; 500$ и 1000 мкс при $P_{err,0}= 0,01; 0,02; 0,05$ и $0,10$ соответственно.



a)

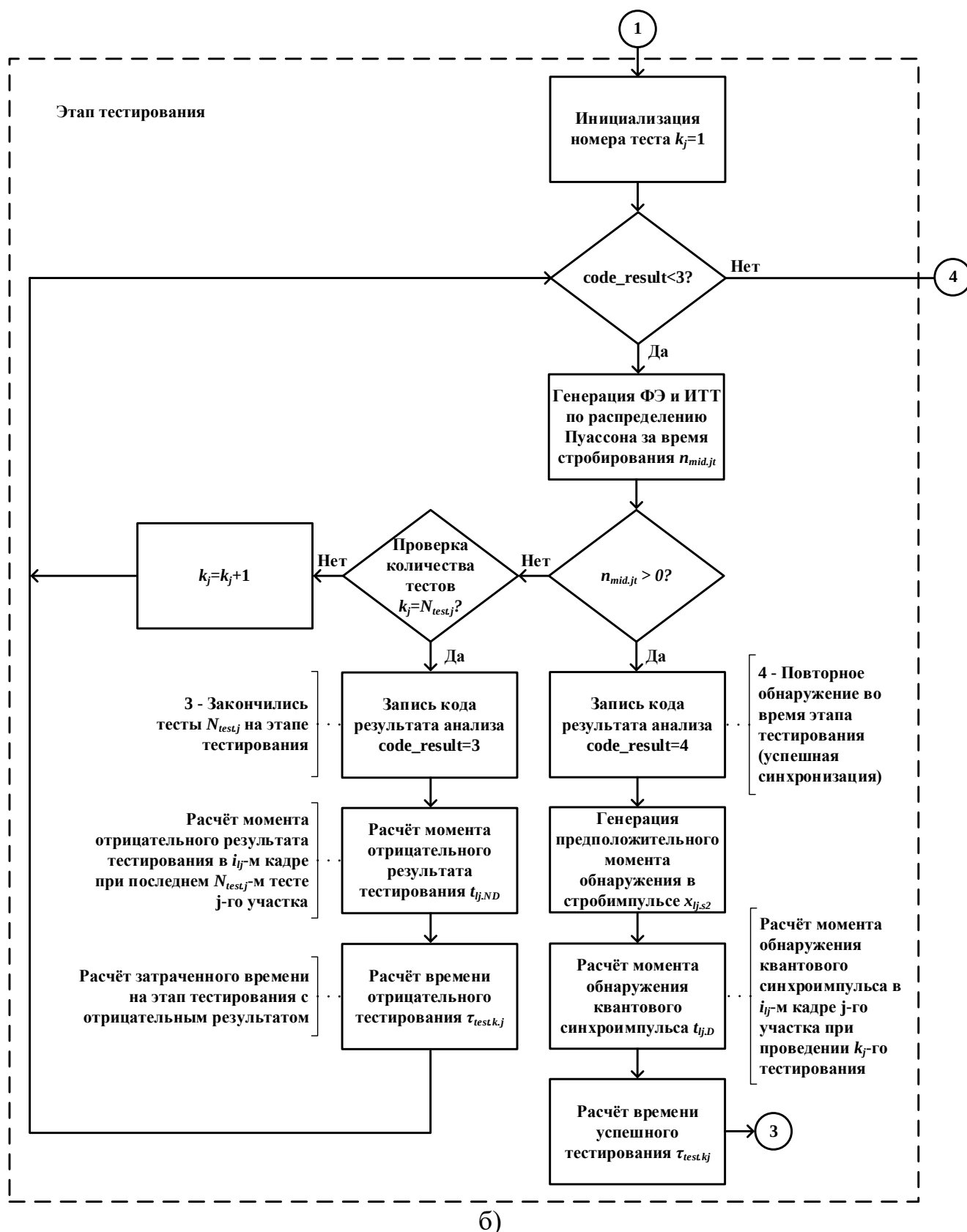


Рисунок 3.10 – Блок-схема двухэтапного алгоритма синхронизации

В таблицу 3.12 сведены результаты моделирования двухэтапного алгоритма синхронизации.

Таблица 3.12 – Результаты моделирования двухэтапного алгоритма синхронизации, количество экспериментов 1000000

Параметры алгоритма синхронизации		$P_{err.0}$			
		0,01	0,02	0,05	0,10
Среднее число тестов при успешном тестировании		13,25	15,63	21,72	30,86
СКО числа тестов при успешном тестировании		12,51	14,72	20,42	29,40
Среднее время успешного тестирования, мс		1,11	2,6	10,86	30,86
Среднее время синхронизации, мс		2,16	5,14	21,67	62,57
СКО времени синхронизации, мс		1,52	3,7	16,72	54,17
Вероятность синхронизации в j-ом участке ВОЛС, %	j=1	99,4691	98,8945	97,2372	94,4363
	j=2	0,5290	1,0931	2,6841	5,2466
	j=3	0,0019	0,0124	0,0774	0,2995
	j=4	0,00	0,00	0,0013	0,0167
	j=5...10	0,00	0,00	0,00	0,00

Анализируя полученные результаты моделирования, отметим, среднее число тестов и среднее время при успешном тестировании наиболее близки к соответствующим значениям, полученным ранее при теоретических расчётах для 1-го участка (см. таблицы 3.8 и 3.9). Это обусловлено тем, что наибольшая вероятность синхронизации станций в 1-м участке. Так, при $P_{err.0}=0,01$ отклонение среднего числа тестов при успешном тестировании составляет 0,15% от теоретических расчётов, а отклонение среднего времени успешного тестирования равно 0,9%. При ухудшении вероятности ошибки синхронизации $P_{err.0}=0,10$ отклонение среднего числа тестов при успешном тестировании составляет 5,9% от теоретических расчётов, а отклонение среднего времени успешного тестирования равно 6%.

Вероятность синхронизации в 1-м участке ВОЛС равна 99,47; 98,89; 97,24 и 94,44 при $P_{err.0}=0,01$; 0,02; 0,05 и 0,10 соответственно. Таким образом, при $P_{err.0}=0,01$ из 1000000 экспериментов 994691 эксперимент завершился синхронизацией в 1-м участке, 5290 экспериментов завершились синхронизацией во 2-м участке и 19 экспериментов – в 3-м участке. Так, при $P_{err.0}=0,01$ процесс синхронизации станций завершается не далее 3-го участка. При ухудшении вероятности ошибки синхронизации до $P_{err.0}=0,10$ процесс синхронизации

завершается не далее 5-го участка, при этом из 1000000 экспериментов 944363 эксперимента завершились синхронизацией в 1-м участке, 52466 экспериментов завершились синхронизацией во 2-м участке, 2995 экспериментов – в 3-м участке, 167 экспериментов – в 4-м участке и 9 экспериментов – в 5-м участке. Отметим, что отклонение вероятности синхронизации в 1-м участке от теоретических расчётов не превышает 5%, составляя соответственно 0,5; 0,9; 2,3 и 4,7% при $P_{err.0}=0,01$; 0,02; 0,05 и 0,10. Это подтверждает возможность использовать ранее полученные аналитические выражения.

Среднее время синхронизации значительно увеличивается при ухудшении требований к ошибке синхронизации $P_{err.0}$. Так, при увеличении вероятности ошибки синхронизации в 10 раз с $P_{err.0}=0,01$ до $P_{err.0}=0,10$ среднее время синхронизации увеличивается более чем в 28,9 раза (62,57 мс против 2,16 мс).

Резюме. Посредством моделирования двухэтапного алгоритма синхронизации станций системы КРК с разбиением ВОЛС на участки с убывающей длиной определены среднее число тестов и среднее время успешного тестирования, вероятность и среднее время синхронизации с дисперсией и СКО. Результаты расчёта среднего числа тестов сигнального интервала и, следовательно, среднего времени успешного тестирования наиболее близки к теоретическим расчётам для первого участка ВОЛС, что обусловлено высокой вероятностью синхронизации в первом участке (более 99% при $P_{err.0}=0,01$ и более 94% при $P_{err.0}=0,10$). При ухудшении вероятности ошибки синхронизации до $P_{err.0}=0,10$ процесс синхронизации завершается не далее 5-го участка, причём вероятности синхронизации в 4-м и 5-м участках близки к нулю и равны 0,0167 и 0,0009% соответственно.

3.10 Выводы к главе 3

Предложена методика разбиения ВОЛС на участки с убывающей длиной при обеспечении вероятности ошибки синхронизации на верхней границе любого участка не выше допустимого значения для двухэтапного временного алгоритма синхронизации станций системы КРК. Получены аналитические выражения для разбиения ВОЛС на участки с убывающей длиной. Разбиение ВОЛС на участки с

убывающей длиной позволяет значительно уменьшить влияние ИТТ ОЛФД за время анализа участка. Благодаря этому увеличивается отношение сигнал/шум.

Полученные аналитические выражения для расчёта вероятностных, временных и энергетических характеристик предложенного двухэтапного алгоритма синхронизации станций доказывают эффективность алгоритма при протяжённости ВОЛС более 80 км при вероятности ошибки синхронизации $P_{err.0}=0,10$, по сравнению с алгоритмом-аналогом, в котором протяжённость ВОЛС не превышает 40 км [104].

Исследована зависимость протяжённости ВОЛС от вероятности ошибки синхронизации. Так, при ухудшении вероятности ошибки синхронизации в 10 раз (с $P_{err.0}=0,01$ до $P_{err.0}=0,10$) протяжённость ВОЛС увеличивается в 2,5 раза (82 км против 33,4 км). Ограничение на протяжённость ВОЛС также накладывает частота генерации ИТТ, причём при ухудшении характеристик ОЛФД (увеличении частоты генерации ИТТ) протяжённость ВОЛС значительно сокращается – увеличение частоты генерации ИТТ в ~10 раз (с 6 до 50 Гц) при гарантии вероятности ошибки синхронизации $P_{err.0}=0,10$ приводит к сокращению длины ВОЛС в 2,2 раза (81,96 км против 37,53 км, см. табл. 3.5). Ещё более значительные ограничения на разнесение станций наблюдаются при ужесточении требований к вероятности ошибки синхронизации – при $P_{err.0}=0,01$ сокращение длины ВОЛС составляет 4,3 раза (33,35 км против 7,72 км).

Проведено моделирование предложенного двухэтапного алгоритма синхронизации приёмопередающей и кодирующей станций системы КРК, получены временные и вероятностные характеристики алгоритма. При ухудшении требований к вероятности ошибки синхронизации на порядок (с $P_{err.0}=0,01$ до $P_{err.0}=0,10$) среднее время вхождения в синхронизм увеличивается в десятки раз (в 28,9 раза – 62,57 мс против 2,16 мс). Ужесточение требований к вероятности ошибки синхронизации позволяет достичь синхронизации станций в 1-м участке с вероятностью более 99%. Сравнительный анализ полученных результатов с теоретическими расчётами показывает на незначительное отклонение вероятности синхронизации в 1-м участке (не более 5%) при различных допустимых

вероятностях ошибки синхронизации, что указывает на правильность полученных аналитических выражений для предложенного алгоритма синхронизации.

Результаты проведённых исследований отражены в статьях [16, 25, 26] и апробированы на научно-технических конференциях: 13th International Conference on Security of Information and Networks (SIN 2020), 4-7 ноября 2020, Стамбул, Турция; The 3rd International Conference on System Reliability and Safety Engineering (SRSE 2021), 26-28 ноября 2021, Харбин, Китай.

4. СТАТИСТИЧЕСКАЯ ОЦЕНКА ВРЕМЕНИ ДВУХЭТАПНОЙ СИНХРОНИЗАЦИИ ПРИЁМОПЕРЕДАЮЩЕЙ И КОДИРУЮЩЕЙ СТАНЦИЙ СИСТЕМЫ КРК

4.1 Постановка задачи статистической оценки времени двухэтапной синхронизации приёмопередающей и кодирующей станций СКРК

В результате проведённых исследований получены аналитические выражения (3.33)-(3.35) для расчёта среднего времени синхронизации станций. Отметим, данные выражения являются приближёнными из-за ряда допущений: фотон или ИТТ регистрируются в конкретном кадре на этапе поиска или при конкретном тесте в j -м сигнальном участке.

Синхронизация зависит от случайного момента регистрации фотона в j -м участке ВОЛС и случайного номера кадра на этапе поиска, от случайного момента регистрации фотона и случайного номера теста на этапе тестирования, а также от вероятности его обнаружения при наличии ИТТ. Следовательно, время синхронизации есть случайная величина. Поэтому, кроме среднего времени вхождения в синхронизм необходимо также определить рассеивание значений случайной величины относительно её математического ожидания: дисперсию и среднеквадратичное отклонение (СКО). Для нахождения этих характеристик применим методику, описанную в [111, 112, 113]. Так как процесс поиска синхроимпульса является стохастическим процессом, то он может быть описан стохастическим или вероятностным деревом.

Отметим, процесс поиска синхроимпульса, или синхронизация станций системы КРК, характеризуется множеством возможных состояний (начало синхронизации, этап поиска, этап тестирования и т.д.), и в определённый момент времени принимает только одно из указанных состояний. С течением времени процесс переходит из одного состояния в другое с вероятностью, зависящей только от состояния, из которого начался рассматриваемый переход. Данное определение является определением конечной марковской цепи, с помощью которой могут быть

получены аналитические выражения для расчёта среднего времени вхождения в синхронизм станций системы КРК, а также дисперсии и СКО. В связи с тем, что процесс поиска заканчивается переходом в конечное состояние (синхронизация станций), то марковская цепь будет являться марковской цепью с поглощением.

4.2 Диаграмма состояний и переходов для случайного поиска

Главным отличием предлагаемого алгоритма от алгоритма-аналога [98] является возможность увеличения протяжённости ВОЛС более 80 км.

Рассчитаем среднее время, необходимое для синхронизации станций, для предлагаемого алгоритма графоаналитическим методом при произвольном количестве участков, кадров и тестов. Для этого воспользуемся диаграммой состояний и переходов на рисунке 4.1, где

$a_{1,j.1} \dots a_{1,j.N_j}$ – непоглощающее состояние. Поиск фотонного импульса, анализ временного кадра длительностью T_s ;

$a_{2,j.1} \dots a_{2,j.N_{test,j}}$ – непоглощающее состояние. Режим тестирования при правильном обнаружении фотонного импульса;

a_3 – поглощающее состояние. Успешная синхронизация станций;

$P_{11,j.i_{lj}}$ – вероятность отсутствия регистрации фотона и/или ИТТ на этапе поиска в течение i_{lj} -го кадра. Если кадр последний $i_{lj} = N_j$, переход к анализу следующего участка. Если участок последний, то переход к анализу 1-го участка;

$P_{12,j.i_{lj}}$ – вероятность регистрации фотона и/или ИТТ на этапе поиска в течение i_{lj} -го кадра и переход к этапу тестирования (состояние a_2);

$P_{23,j.k_j}$ – вероятность повторной регистрации фотона за длительность строб-импульса τ_{strob} на этапе тестирования в течение k_j -го теста. Процесс грубой синхронизации станций успешно завершён (состояние a_3);

$Q_{23,j.k_j}$ – вероятность отсутствия повторной регистрации фотона за длительность строб-импульса τ_{strob} на этапе тестирования за k_j тестов. Если тест последний $k_j = N_{test,j}$, то переход к анализу следующего участка. Если участок последний, то переход к анализу 1-го участка. Длительность импульса стробирования $\tau_{strob} = 2\tau_s + 2\Delta T_s$.

Отметим, что состояние марковской цепи называется поглощающим, если из него невозможно перейти ни в какое другое состояние.

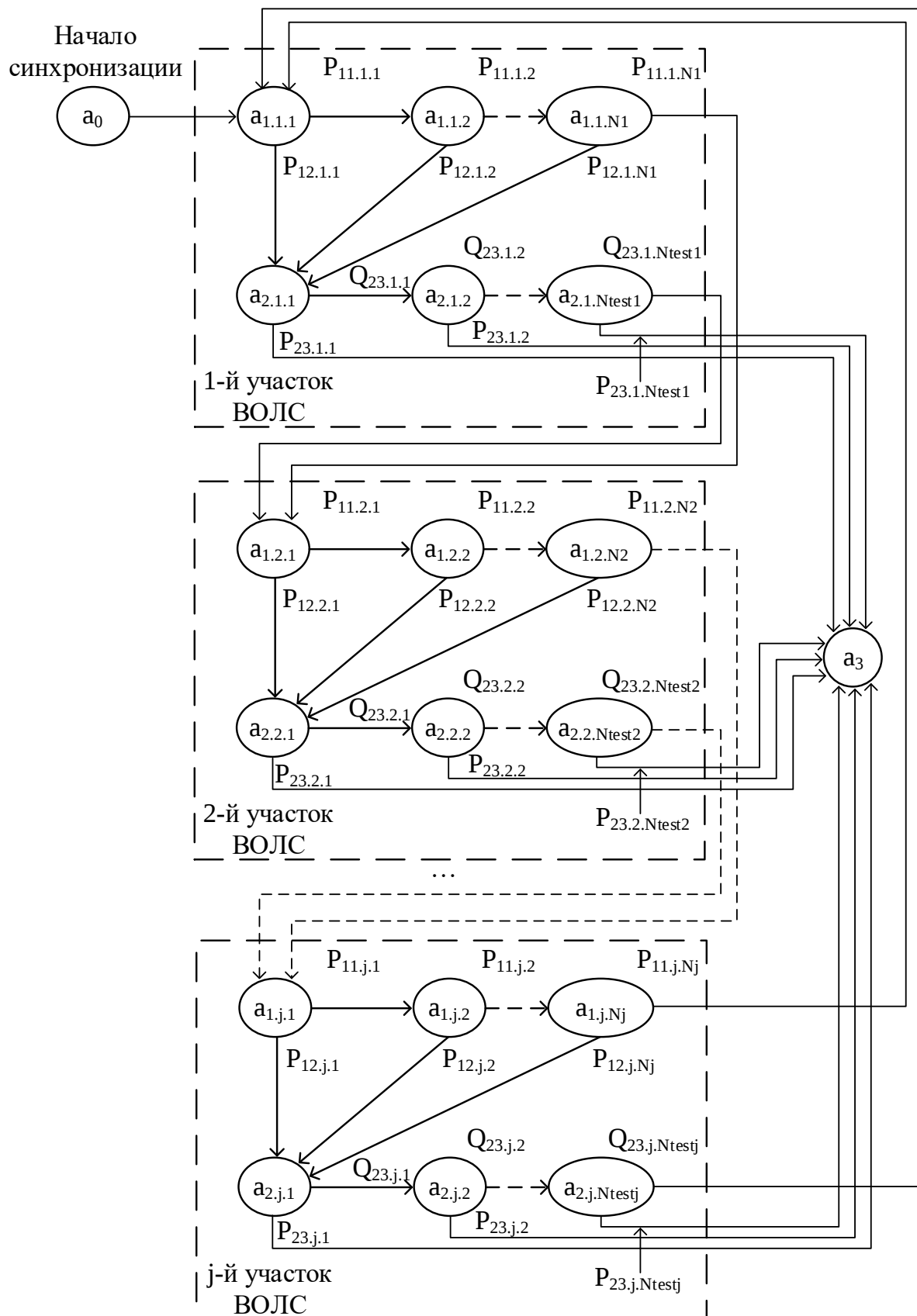


Рисунок 4.1 – Диаграмма состояний и переходов для случайного поиска

Отметим, вероятности $P_{11.j.i_{lj}}$ и $P_{12.j.i_{lj}}$, $P_{23.j.kj}$ и $Q_{23.j.kj}$ зависят только от средних чисел фотонов в фотонном импульсе $\overline{n_{s,j}}$, ИТТ $\overline{n_{DCR,j}}$ и $\overline{n_{strob,j}}$, которые изменяются лишь при переходе к анализу следующего участка. Указанные вероятности постоянны внутри участка:

$$\begin{aligned} P_{11.j.1} &= P_{11.j.2} = \dots = P_{11.j.N_j} = P_{11.j} ; \\ P_{12.j.1} &= P_{12.j.2} = \dots = P_{12.j.N_j} = P_{12.j} ; \\ P_{23.j.1} &= P_{23.j.2} = \dots = P_{23.j.N_{test,j}} = P_{23.j} ; \\ Q_{23.j.1} &= Q_{23.j.2} = \dots = Q_{23.j.N_{test,j}} = Q_{23.j} . \end{aligned}$$

Вероятность $P_{11.j}$ рассчитывается по (3.39). Причём $P_{12.j} = 1 - P_{11.j}$. Вероятность отсутствия повторной регистрации фотона за длительность строб-импульса равна $Q_{23.j} = e^{-\overline{n_{strob,j}}}$. Среднее число регистрируемых фотонов за длительность фотонного импульса $\overline{n_{s,j}}$ при анализе j -го участка может быть найдено по (3.37).

Резюме. Построена диаграмма состояний и переходов для случайного поиска для предложенного двухэтапного алгоритма синхронизации станций с разбиением ВОЛС на участки с убывающей длиной. Определены состояния системы, а также вероятности переходов между ними.

4.3 Определение статистических характеристик двухэтапного алгоритма графоаналитическим методом

Проведём расчёт среднего времени синхронизации при различных комбинациях количества кадров N_j , тестов $N_{test,j}$ и участков N_{FOL} .

Раскроем методику расчёта статистических характеристик при допущении, что ВОЛС состоит из одного участка $N_{FOL} = 1$. Допустимые количество кадров и тестов в участке соответственно равны $N_1 = 1$ и $N_{test,1} = 1$.

Для нахождения статистических характеристик поиска образуем стохастическую матрицу вероятностей перехода между состояниями:

$$P = \begin{pmatrix} P_{11.1} & P_{12.1} & 0 \\ Q_{23.1} & 0 & P_{23.1} \\ 0 & 0 & 0 \end{pmatrix}. \quad (4.1)$$

Первый столбец соответствует состоянию $a_{1.1}$, второй – $a_{2.1}$, третий – a_3 . Аналогично первая строка соответствует состоянию $a_{1.1}$, вторая – $a_{2.1}$, третья – a_3 .

Отметим, что сумма вероятностей в каждой строке равна 1.

Среднее число проходов процесса через непоглощающее состояние a_j при исходном непоглощающем состоянии a_i определяется выражением:

$$T = (I - Q)^{-1}, \quad (4.2)$$

где I – единичная матрица, Q – матрица, образованная из матрицы P путём исключения столбцов и строк поглощающих состояний:

$$Q = \begin{pmatrix} P_{11.1} & P_{12.1} \\ Q_{23.1} & 0 \end{pmatrix}. \quad (4.3)$$

Найдём матрицу:

$$A = I - Q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} P_{11.1} & P_{12.1} \\ Q_{23.1} & 0 \end{pmatrix} = \begin{pmatrix} 1 - P_{11.1} & -P_{12.1} \\ -Q_{23.1} & 1 \end{pmatrix}. \quad (4.4)$$

Для нахождения обратной матрицы A^{-1} находим её определитель:

$$|A| = \begin{vmatrix} 1 - P_{11.1} & -P_{12.1} \\ -Q_{23.1} & 1 \end{vmatrix} = 1 - P_{11.1} - P_{12.1}Q_{23.1}. \quad (4.5)$$

Обратная матрица A^{-1} связана с транспонированной матрицей алгебраических дополнений A_d^T :

$$A^{-1} = \frac{1}{|A|} \cdot A_d^T. \quad (4.6)$$

Для определения транспонированной матрицы алгебраических дополнений находим матрицу миноров.

$$M = \begin{pmatrix} 1 & -Q_{23.1} \\ -P_{12.1} & 1 - P_{11.1} \end{pmatrix}, \quad (4.7)$$

матрицу алгебраических дополнений

$$A_d = \begin{pmatrix} 1 & Q_{23.1} \\ P_{12.1} & 1 - P_{11.1} \end{pmatrix} \quad (4.8)$$

и транспонируем матрицу алгебраических дополнений

$$A_d^T = \begin{pmatrix} 1 & P_{12.1} \\ Q_{23.1} & 1 - P_{11.1} \end{pmatrix}. \quad (4.9)$$

Следовательно, теперь можно вычислить обратную матрицу

$$T = A^{-1} = \begin{pmatrix} -\frac{1}{P_{11.1} + P_{12.1}Q_{23.1} - 1} & -\frac{P_{12.1}}{P_{11.1} + P_{12.1}Q_{23.1} - 1} \\ -\frac{Q_{23.1}}{P_{11.1} + P_{12.1}Q_{23.1} - 1} & \frac{P_{11.1} - 1}{P_{11.1} + P_{12.1}Q_{23.1} - 1} \end{pmatrix}. \quad (4.10)$$

Таким образом, если процесс начинается с непоглощающего состояния $a_{1.1}$, то он пройдет непоглощающее состояние $a_{2.1}$ в среднем $P_{12.1}/(1 - P_{11.1} - P_{12.1}Q_{23.1})$ раз.

Дисперсия числа проходов между состояниями определяется выражением

$$\{D_i[n_j]\} = T \cdot (2T_d - I) - T_q, \quad (4.11)$$

где T_d – диагональная матрица T , T_q – квадратная матрица T .

Тогда

$$\{D_i[n_j]\} = \begin{pmatrix} \frac{\frac{2}{P_{11.1} + P_{12.1}Q_{23.1} - 1} + 1}{P_{11.1} + P_{12.1}Q_{23.1} - 1} - \frac{1}{(P_{11.1} + P_{12.1}Q_{23.1} - 1)^2} & -\frac{P_{12.1}^2}{(P_{11.1} + P_{12.1}Q_{23.1} - 1)^2} - \frac{P_{12.1} \cdot \left(\frac{2 \cdot P_{11.1} - 2}{P_{11.1} + P_{12.1}Q_{23.1} - 1} - 1\right)}{P_{11.1} + P_{12.1}Q_{23.1} - 1} \\ \frac{Q_{23.1} \cdot \left(\frac{2}{P_{11.1} + P_{12.1}Q_{23.1} - 1} + 1\right)}{P_{11.1} + P_{12.1}Q_{23.1} - 1} - \frac{Q_{23.1}^2}{(P_{11.1} + P_{12.1}Q_{23.1} - 1)^2} & \frac{(P_{11.1} - 1) \cdot \left(\frac{2 \cdot P_{11.1} - 2}{P_{11.1} + P_{12.1}Q_{23.1} - 1} - 1\right)}{P_{11.1} + P_{12.1}Q_{23.1} - 1} - \frac{(P_{11.1} - 1)^2}{(P_{11.1} + P_{12.1}Q_{23.1} - 1)^2} \end{pmatrix}.$$

Если процесс начинается в непоглощающем состоянии $a_{1.1}$, то дисперсия числа проходов процесса через непоглощающее состояние $a_{2.1}$ равна

$$\{D_1[n_2]\} = -\frac{P_{12.1}^2}{(P_{11.1} + P_{12.1}Q_{23.1} - 1)^2} - \frac{P_{12.1} \cdot \left(\frac{2 \cdot P_{11.1} - 2}{P_{11.1} + P_{12.1}Q_{23.1} - 1} - 1\right)}{P_{11.1} + P_{12.1}Q_{23.1} - 1}.$$

Среднее число шагов m , которое затрачивается при переходе из непоглощающего состояния a_j в поглощающее состояние a_i , равно:

$$m = T \cdot B, \quad (4.12)$$

где B – вектор-столбец, все компоненты которого равны единице.

Таким образом, среднее число шагов будет равно

$$m = \begin{pmatrix} m_{13} \\ m_{23} \end{pmatrix} = \begin{pmatrix} -P_{12.1}/(P_{11.1} + P_{12.1}Q_{23.1} - 1) - 1/(P_{11.1} + P_{12.1}Q_{23.1} - 1) \\ (P_{11.1} - 1)/(P_{11.1} + P_{12.1}Q_{23.1} - 1) - Q_{23.1}/(P_{11.1} + P_{12.1}Q_{23.1} - 1) \end{pmatrix}.$$

Элемент первой строки равен числу шагов перехода из непоглощающего состояния $a_{1.1}$ в поглощающее a_3 , элемент второй строки – из непоглощающего состояния $a_{2.1}$ в поглощающее a_3 .

Следовательно, среднее число шагов для перехода из состояния начала синхронизации $a_{1.1}$ в состояние успешной синхронизации a_3 равно

$$m = -\frac{P_{12.1}}{P_{11.1}+P_{12.1}Q_{23.1}-1} - \frac{1}{P_{11.1}+P_{12.1}Q_{23.1}-1} = -\frac{1+P_{12.1}}{P_{11.1}+P_{12.1}Q_{23.1}-1}. \quad (4.14)$$

Среднее время синхронизации станций равно $\overline{\tau_{sync}} = m \cdot T_s$.

Дисперсия числа шагов, затрачиваемых на переход процесса из непоглощающего состояния в поглощающее, определяется выражением

$$\{D_i[\alpha_m]\} = (2T - I)m - m_{KB}, \quad (4.13)$$

где α_m – число шагов, затрачиваемых на переход из непоглощающего состояния a_i в поглощающее, m_{KB} – квадратный вектор-столбец m .

Тогда

$$\{D_i[\alpha_m]\} = \begin{pmatrix} d_{13} \\ d_{23} \end{pmatrix} = \begin{pmatrix} \frac{P_{11.1}+P_{12.1}[1+3Q_{23.1}-P_{11.1}+P_{12.1}(Q_{23.1}-1)]}{(P_{12.1}Q_{23.1}+P_{11.1}-1)^2} \\ \frac{Q_{23.1}[1+P_{11.1}-Q_{23.1}+P_{12.1}(Q_{23.1}-P_{11.1}+3)]}{(P_{12.1}Q_{23.1}+P_{11.1}-1)^2} \end{pmatrix},$$

где d_{13} – дисперсия числа шагов, затрачиваемых на переход процесса из непоглощающего состояния $a_{1.1}$ в поглощающее a_3 , d_{23} – из непоглощающего состояния $a_{2.1}$ в поглощающее a_3 .

Отличительной особенностью предлагаемого алгоритма синхронизации является разбиение ВОЛС на участки с убывающей длиной и их последовательный анализ до момента установления синхронизации.

Случай 1. Пусть ВОЛС состоит из двух участков $N_{FOL} = 2$. Допустимые количество кадров и тестов в первом и втором участках соответственно равны $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 1$ и $N_{test.2} = 1$. Диаграмму состояний и переходов представим в табличном виде:

	$a_{1.1.1}$	$a_{1.1.2}$	$a_{1.1.3}$	$a_{2.1.1}$	$a_{2.1.2}$	$a_{2.1.3}$	$a_{1.2.1}$	$a_{2.2.1}$	a_3
$a_{1.1.1}$		$P_{11.1}$		$P_{12.1}$					
$a_{1.1.2}$			$P_{11.1}$	$P_{12.1}$					
$a_{1.1.3}$				$P_{12.1}$			$P_{11.1}$		
$a_{2.1.1}$					$Q_{23.1}$				$P_{23.1}$
$a_{2.1.2}$						$Q_{23.1}$			$P_{23.1}$
$a_{2.1.3}$							$Q_{23.1}$		$P_{23.1}$
$a_{1.2.1}$	$P_{11.2}$							$P_{12.2}$	
$a_{2.2.1}$	$Q_{23.2}$								$P_{23.2}$
a_3									

Представим среднее число шагов для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 в виде дроби $m_{13} = m_{13.n}/m_{13.d}$, где

$$m_{13.n} = (P_{11.1}^2 + P_{11.1} + 1)[1 + P_{12.1}(Q_{23.1}^2 + Q_{23.1} + 1) + P_{12.1}Q_{23.1}^3(1 + P_{12.2})] \rightarrow$$

$$\leftarrow +P_{11.1}^3(1 + P_{12.2}); \quad (4.15)$$

$$m_{13.d} = 1 - (P_{11.2} + P_{12.2}Q_{23.2}) \cdot [P_{11.1}^3 + P_{12.1}Q_{23.1}^3(P_{11.1}^2 + P_{11.1} + 1)]. \quad (4.16)$$

При произвольных значениях N_1 и $N_{test.1}$ получим

$$m_{13.n} = \sum_{k=1}^{N_1} P_{11.1}^{k-1} [1 + P_{12.1} \sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1} + P_{12.1}Q_{23.1}^{N_{test.1}}(1 + P_{12.2})] \rightarrow$$

$$\leftarrow +P_{11.1}^{N_1}(1 + P_{12.2}); \quad (4.17)$$

$$m_{13.d} = 1 - (P_{11.2} + P_{12.2}Q_{23.2})[P_{11.1}^{N_1} + P_{12.1}Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}]. \quad (4.18)$$

Случай 2. Пусть ВОЛС состоит из двух участков $N_{FOL} = 2$. Допустимые количество кадров и тестов в первом и втором участках соответственно равны $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 1$ и $N_{test.2} = 2$. Диаграмму состояний и переходов представим в табличном виде:

	$a_{1.1.1}$	$a_{1.1.2}$	$a_{1.1.3}$	$a_{2.1.1}$	$a_{2.1.2}$	$a_{2.1.3}$	$a_{1.2.1}$	$a_{2.2.1}$	$a_{2.2.2}$	a_3
$a_{1.1.1}$		$P_{11.1}$		$P_{12.1}$						
$a_{1.1.2}$			$P_{11.1}$	$P_{12.1}$						
$a_{1.1.3}$				$P_{12.1}$			$P_{11.1}$			
$a_{2.1.1}$					$Q_{23.1}$					$P_{23.1}$
$a_{2.1.2}$						$Q_{23.1}$				$P_{23.1}$
$a_{2.1.3}$							$Q_{23.1}$			$P_{23.1}$
$a_{1.2.1}$	$P_{11.2}$							$P_{12.2}$		
$a_{2.2.1}$									$Q_{23.2}$	$P_{23.2}$
$a_{2.2.2}$	$Q_{23.2}$									$P_{23.2}$
a_3										

Среднее число шагов для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 равно $m_{13} = m_{13.n}/m_{13.d}$,

$$m_{13.n} = (1 + P_{11.1} + P_{11.1}^2) \rightarrow$$

$$\leftarrow \cdot [1 + P_{12.1}(1 + Q_{23.1} + Q_{23.1}^2) + P_{12.1}Q_{23.1}^3(1 + P_{12.2}(1 + Q_{23.2}))] \rightarrow \quad (4.19)$$

$$\leftarrow +P_{11.1}^3(1 + P_{12.2}(1 + Q_{23.2}));$$

$$m_{13.d} = 1 - (1 + P_{11.1} + P_{11.1}^2)[P_{12.1}Q_{23.1}^3(P_{11.2} + P_{12.2}Q_{23.2}^2)] \rightarrow$$

$$\leftarrow -P_{11.1}^3(P_{11.2} + P_{12.2}Q_{23.2}^2). \quad (4.20)$$

При произвольных значениях N_1 и $N_{test.1}$ получим

$$m_{13.n} = \sum_{k=1}^{N_1} P_{11.1}^{k-1} [1 + P_{12.1} \sum_{k=1}^{N_{test1}} Q_{23.1}^{k-1} + P_{12.1} Q_{23.1}^{N_{test1}} (1 + P_{12.2} (1 + Q_{23.2}))] \rightarrow$$

$$\leftarrow + P_{11.1}^{N_1} (1 + P_{12.2} (1 + Q_{23.2})); \quad (4.21)$$

$$m_{13.d} = 1 - \sum_{k=1}^{N_1} P_{11.1}^{k-1} [P_{12.1} Q_{23.1}^{N_{test1}} (P_{11.2} + P_{12.2} Q_{23.2}^2)] \rightarrow$$

$$\leftarrow - P_{11.1}^{N_1} (P_{11.2} + P_{12.2} Q_{23.2}^2). \quad (4.22)$$

Случай 3. Пусть ВОЛС состоит из двух участков $N_{FOL} = 2$. Допустимые количество кадров и тестов в первом и втором участках соответственно равны $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 1$ и $N_{test.2} = 3$. Диаграмму состояний и переходов представим в табличном виде:

	$a_{1.1.1}$	$a_{1.1.2}$	$a_{1.1.3}$	$a_{2.1.1}$	$a_{2.1.2}$	$a_{2.1.3}$	$a_{1.2.1}$	$a_{2.2.1}$	$a_{2.2.2}$	$a_{2.2.3}$	a_3
$a_{1.1.1}$		$P_{11.1}$		$P_{12.1}$							
$a_{1.1.2}$			$P_{11.1}$	$P_{12.1}$							
$a_{1.1.3}$				$P_{12.1}$			$P_{11.1}$				
$a_{2.1.1}$					$Q_{23.1}$						$P_{23.1}$
$a_{2.1.2}$						$Q_{23.1}$					$P_{23.1}$
$a_{2.1.3}$							$Q_{23.1}$				$P_{23.1}$
$a_{1.2.1}$	$P_{11.2}$							$P_{12.2}$			
$a_{2.2.1}$									$Q_{23.2}$		$P_{23.2}$
$a_{2.2.2}$										$Q_{23.2}$	$P_{23.2}$
$a_{2.2.3}$	$Q_{23.2}$										$P_{23.2}$
a_3											

Среднее число шагов для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 равно $m_{13} = m_{13.n}/m_{13.d}$,

$$m_{13.n} = (1 + P_{11.1} + P_{11.1}^2) \rightarrow$$

$$\leftarrow \cdot [1 + P_{12.1} (1 + Q_{23.1} + Q_{23.1}^2) + P_{12.1} Q_{23.1}^3 (1 + P_{12.2} (1 + Q_{23.2} + Q_{23.2}^2))] \rightarrow$$

$$\leftarrow + P_{11.1}^3 (1 + P_{12.2} (1 + Q_{23.2} + Q_{23.2}^2)); \quad (4.23)$$

$$m_{13.d} = 1 - (1 + P_{11.1} + P_{11.1}^2) [P_{12.1} Q_{23.1}^3 (P_{11.2} + P_{12.2} Q_{23.2}^3)] \rightarrow$$

$$\leftarrow - P_{11.1}^3 (P_{11.2} + P_{12.2} Q_{23.2}^3). \quad (4.24)$$

При произвольных значениях N_1 , $N_{test.1}$ и $N_{test.2}$ получим

$$m_{13.n} = \sum_{k=1}^{N_1} P_{11.1}^{k-1} \rightarrow$$

$$\leftarrow \cdot [1 + P_{12.1} \sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1} + P_{12.1} Q_{23.1}^{N_{test.1}} (1 + P_{12.2} \sum_{k=1}^{N_{test.2}} Q_{23.2}^{k-1})] \rightarrow \quad (4.25)$$

$$\leftarrow + P_{11.1}^{N_1} (1 + P_{12.2} \sum_{k=1}^{N_{test.2}} Q_{23.2}^{k-1});$$

$$m_{13.d} = 1 - \sum_{k=1}^{N_1} P_{11.1}^{k-1} [P_{12.1} Q_{23.1}^{N_{test.1}} (P_{11.2} + P_{12.2} Q_{23.2}^{N_{test.2}})] \rightarrow$$

$$\leftarrow -P_{11.1}^{N_1}(P_{11.2} + P_{12.2}Q_{23.2}^{N_{test.2}}). \quad (4.26)$$

Случай 4. Диаграмму состояний и переходов для $N_{FOL} = 2$, $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 2$ и $N_{test.2} = 1$ представим в табличном виде:

	$a_{1.1.1}$	$a_{1.1.2}$	$a_{1.1.3}$	$a_{2.1.1}$	$a_{2.1.2}$	$a_{2.1.3}$	$a_{1.2.1}$	$a_{1.2.2}$	$a_{2.2.1}$	a_3
$a_{1.1.1}$		$P_{11.1}$		$P_{12.1}$						
$a_{1.1.2}$			$P_{11.1}$	$P_{12.1}$						
$a_{1.1.3}$				$P_{12.1}$			$P_{11.1}$			
$a_{2.1.1}$					$Q_{23.1}$					$P_{23.1}$
$a_{2.1.2}$						$Q_{23.1}$				$P_{23.1}$
$a_{2.1.3}$							$Q_{23.1}$			$P_{23.1}$
$a_{1.2.1}$								$P_{11.2}$	$P_{12.2}$	
$a_{1.2.2}$	$P_{11.2}$								$P_{12.2}$	
$a_{2.2.1}$	$Q_{23.2}$									$P_{23.2}$
a_3										

Среднее число шагов для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 равно $m_{13} = m_{13.n}/m_{13.d}$,

$$\begin{aligned} m_{13.n} &= (1 + P_{11.1} + P_{11.1}^2) \rightarrow \\ &\leftarrow [1 + P_{12.1}(1 + Q_{23.1} + Q_{23.1}^2) + P_{12.1}Q_{23.1}^3(1 + P_{11.2})(1 + P_{12.2})] \rightarrow \quad (4.27) \\ &\leftarrow +P_{11.1}^3(1 + P_{11.2})(1 + P_{12.2}); \end{aligned}$$

$$\begin{aligned} m_{13.d} &= 1 - (1 + P_{11.1} + P_{11.1}^2) [P_{12.1}Q_{23.1}^3(P_{11.2}^2 + P_{12.2}Q_{23.2}(1 + P_{11.2}))] \rightarrow \\ &\leftarrow -P_{11.1}^3[P_{11.2}^2 + P_{12.2}Q_{23.2}(1 + P_{11.2})]. \quad (4.28) \end{aligned}$$

При произвольных значениях N_1 и $N_{test.1}$ получим

$$\begin{aligned} m_{13.n} &= \sum_{k=1}^{N_1} P_{11.1}^{k-1} [1 + P_{12.1} (\sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1} + Q_{23.1}^{N_{test.1}}(1 + P_{11.2})(1 + P_{12.2}))] \rightarrow \\ &\leftarrow +P_{11.1}^{N_1}(1 + P_{11.2})(1 + P_{12.2}); \quad (4.29) \end{aligned}$$

$$m_{13.d} = 1 - [P_{11.1}^{N_1} + P_{12.1}Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] [P_{11.2}^2 + P_{12.2}Q_{23.2}(1 + P_{11.2})]. \quad (4.30)$$

Случай 5. Диаграмму состояний и переходов для $N_{FOL} = 2$, $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 2$ и $N_{test.2} = 2$ представим в табличном виде:

	$a_{1.1.1}$	$a_{1.1.2}$	$a_{1.1.3}$	$a_{2.1.1}$	$a_{2.1.2}$	$a_{2.1.3}$	$a_{1.2.1}$	$a_{1.2.2}$	$a_{2.2.1}$	$a_{2.2.2}$	a_3
$a_{1.1.1}$		$P_{11.1}$		$P_{12.1}$							
$a_{1.1.2}$			$P_{11.1}$	$P_{12.1}$							
$a_{1.1.3}$				$P_{12.1}$			$P_{11.1}$				
$a_{2.1.1}$					$Q_{23.1}$						$P_{23.1}$
$a_{2.1.2}$						$Q_{23.1}$					$P_{23.1}$
$a_{2.1.3}$							$Q_{23.1}$				$P_{23.1}$

$a_{1.2.1}$								$P_{11.2}$	$P_{12.2}$		
$a_{1.2.2}$	$P_{11.2}$								$P_{12.2}$		
$a_{2.2.1}$										$Q_{23.2}$	$P_{23.2}$
$a_{2.2.2}$	$Q_{23.2}$										$P_{23.2}$
a_3											

Среднее число шагов для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 равно $m_{13} = m_{13.n}/m_{13.d}$,

$$m_{13.n} = (1 + P_{11.1} + P_{11.1}^2) \rightarrow \leftarrow \cdot \left[1 + P_{12.1} \left((1 + Q_{23.1} + Q_{23.1}^2) + Q_{23.1}^3 (1 + P_{11.2})(1 + P_{12.2}(1 + Q_{23.2})) \right) \right] \rightarrow \quad (4.31)$$

$$\leftarrow + P_{11.1}^3 (1 + P_{11.2})(1 + P_{12.2}(1 + Q_{23.2})) ;$$

$$m_{13.d} = 1 - [P_{11.1}^3 + P_{12.1}Q_{23.1}^3(1 + P_{11.1} + P_{11.1}^2)][P_{11.2}^2 + P_{12.2}Q_{23.2}^2(1 + P_{11.2})] . \quad (4.32)$$

При произвольных значениях N_1 и $N_{test.1}$ получим

$$m_{13.n} = \sum_{k=1}^{N_1} P_{11.1}^{k-1} \rightarrow \leftarrow \cdot \left[1 + P_{12.1} \left(\sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1} + Q_{23.1}^{N_{test.1}} (1 + P_{11.2})(1 + P_{12.2}(1 + Q_{23.2})) \right) \right] \rightarrow \quad (4.33)$$

$$\leftarrow + P_{11.1}^{N_1} (1 + P_{11.2})(1 + P_{12.2}(1 + Q_{23.2})) ;$$

$$m_{13.d} = 1 - [P_{11.1}^{N_1} + P_{12.1}Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}][P_{11.2}^2 + P_{12.2}Q_{23.2}^2(1 + P_{11.2})] . \quad (4.34)$$

Случай 6. Диаграмму состояний и переходов для $N_{FOL} = 2$, $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 2$ и $N_{test.2} = 3$ представим в табличном виде:

	$a_{1.1.1}$	$a_{1.1.2}$	$a_{1.1.3}$	$a_{2.1.1}$	$a_{2.1.2}$	$a_{2.1.3}$	$a_{1.2.1}$	$a_{1.2.2}$	$a_{2.2.1}$	$a_{2.2.2}$	$a_{2.2.3}$	a_3
$a_{1.1.1}$		$P_{11.1}$		$P_{12.1}$								
$a_{1.1.2}$			$P_{11.1}$	$P_{12.1}$								
$a_{1.1.3}$				$P_{12.1}$			$P_{11.1}$					
$a_{2.1.1}$					$Q_{23.1}$							$P_{23.1}$
$a_{2.1.2}$						$Q_{23.1}$						$P_{23.1}$
$a_{2.1.3}$							$Q_{23.1}$					$P_{23.1}$
$a_{1.2.1}$								$P_{11.2}$	$P_{12.2}$			
$a_{1.2.2}$	$P_{11.2}$								$P_{12.2}$			
$a_{2.2.1}$										$Q_{23.2}$		$P_{23.2}$
$a_{2.2.2}$											$Q_{23.2}$	$P_{23.2}$
$a_{2.2.3}$	$Q_{23.2}$											$P_{23.2}$
a_3												

Среднее число шагов для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 равно $m_{13} = m_{13.n}/m_{13.d}$,

$$m_{13.n} = (1 + P_{11.1} + P_{11.1}^2) \rightarrow \leftarrow \cdot \left[1 + P_{12.1} \left((1 + Q_{23.1} + Q_{23.1}^2) + Q_{23.1}^3 (1 + P_{11.2}) (1 + P_{12.2}(1 + Q_{23.2} + Q_{23.2}^2)) \right) \right] \rightarrow \quad (4.35)$$

$$\leftarrow +P_{11.1}^3(1+P_{11.2})(1+P_{12.2}(1+Q_{23.2}+Q_{23.2}^2));$$

$$m_{13.d} = 1 - [P_{11.1}^3 + P_{12.1}Q_{23.1}^3(1+P_{11.1}+P_{11.1}^2)][P_{11.2}^2 + P_{12.2}Q_{23.2}^3(1+P_{11.2})]. \quad (4.36)$$

При произвольных значениях N_1 , $N_{test.1}$ и $N_{test.2}$ получим

$$m_{13.n} = \sum_{k=1}^{N_1} P_{11.1}^{k-1} \rightarrow$$

$$\leftarrow \cdot \left[1 + P_{12.1} \left(\sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1} + Q_{23.1}^{N_{test.1}} (1 + P_{11.2}) (1 + P_{12.2} \sum_{k=1}^{N_{test.2}} Q_{23.2}^{k-1}) \right) \right] \rightarrow \quad (4.37)$$

$$\leftarrow +P_{11.1}^{N_1} (1 + P_{11.2}) (1 + P_{12.2} \sum_{k=1}^{N_{test.2}} Q_{23.2}^{k-1});$$

$$m_{13.d} = 1 - [P_{11.1}^{N_1} + P_{12.1}Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] [P_{11.2}^2 + P_{12.2}Q_{23.2}^{N_{test.2}} (1 + P_{11.2})]. \quad (4.38)$$

Случай 7. Для $N_{FOL} = 2$ и допустимых количествах кадров и тестов в первом и втором участках $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 3$ и $N_{test.2} = 1$ построим диаграмму состояний и переходов в табличном виде:

	$a_{1.1.1}$	$a_{1.1.2}$	$a_{1.1.3}$	$a_{2.1.1}$	$a_{2.1.2}$	$a_{2.1.3}$	$a_{1.2.1}$	$a_{1.2.2}$	$a_{1.2.3}$	$a_{2.2.1}$	a_3
$a_{1.1.1}$		$P_{11.1}$		$P_{12.1}$							
$a_{1.1.2}$			$P_{11.1}$	$P_{12.1}$							
$a_{1.1.3}$				$P_{12.1}$			$P_{11.1}$				
$a_{2.1.1}$					$Q_{23.1}$						$P_{23.1}$
$a_{2.1.2}$						$Q_{23.1}$					$P_{23.1}$
$a_{2.1.3}$							$Q_{23.1}$				$P_{23.1}$
$a_{1.2.1}$								$P_{11.2}$		$P_{12.2}$	
$a_{1.2.2}$									$P_{11.2}$	$P_{12.2}$	
$a_{1.2.3}$	$P_{11.2}$									$P_{12.2}$	
$a_{2.2.1}$	$Q_{23.2}$										$P_{23.2}$
a_3											

Среднее число шагов для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 равно $m_{13} = m_{13.n}/m_{13.d}$,

$$m_{13.n} = (1 + P_{11.1} + P_{11.1}^2) \rightarrow$$

$$\leftarrow \cdot \left[1 + P_{12.1} [1 + Q_{23.1} + Q_{23.1}^2 + Q_{23.1}^3(1 + P_{12.2})(1 + P_{11.2} + P_{11.2}^2)] \right] \rightarrow \quad (4.39)$$

$$\leftarrow +P_{11.1}^3(1 + P_{12.2})(1 + P_{11.2} + P_{11.2}^2);$$

$$m_{13.d} = 1 - [P_{11.1}^3 + P_{12.1}Q_{23.1}^3(1 + P_{11.1} + P_{11.1}^2)] \rightarrow$$

$$\leftarrow \cdot [P_{11.2}^3 + P_{12.2}Q_{23.2}(1 + P_{11.2} + P_{11.2}^2)]. \quad (4.40)$$

При произвольных значениях N_1 и $N_{test.1}$ получим

$$m_{13.n} = \sum_{k=1}^{N_1} P_{11.1}^{k-1} \rightarrow$$

$$\leftarrow \cdot \left[1 + P_{12.1} \left[\sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1} + Q_{23.1}^{N_{test.1}} (1 + P_{12.2}) (1 + P_{11.2} + P_{11.2}^2) \right] \right] \rightarrow \quad (4.41)$$

$$\leftarrow + P_{11.1}^{N_1} (1 + P_{12.2}) (1 + P_{11.2} + P_{11.2}^2);$$

$$m_{13.d} = 1 - \left[P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1} \right] \rightarrow$$

$$\leftarrow \cdot \left[P_{11.2}^3 + P_{12.2} Q_{23.2} (1 + P_{11.2} + P_{11.2}^2) \right]. \quad (4.42)$$

Случай 8. Для $N_{FOL} = 2$, $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 3$ и $N_{test.2} = 2$ среднее число шагов для перехода из состояния $a_{1.1.1}$ в состояние успешной синхронизации a_3 равно $m_{13} = m_{13.n}/m_{13.d}$,

$$m_{13.n} = (1 + P_{11.1} + P_{11.1}^2) \rightarrow$$

$$\leftarrow \cdot \left[1 + P_{12.1} \left[1 + Q_{23.1} + Q_{23.1}^2 + Q_{23.1}^3 [1 + P_{12.2} (1 + Q_{23.2})] (1 + P_{11.2} + P_{11.2}^2) \right] \right] \rightarrow \quad (4.43)$$

$$\leftarrow + P_{11.1}^3 [1 + P_{12.2} (1 + Q_{23.2})] (1 + P_{11.2} + P_{11.2}^2);$$

$$m_{13.d} = 1 - \left[P_{11.1}^3 + P_{12.1} Q_{23.1}^3 (1 + P_{11.1} + P_{11.1}^2) \right] \rightarrow$$

$$\leftarrow \cdot \left[P_{11.2}^3 + P_{12.2} Q_{23.2}^2 (1 + P_{11.2} + P_{11.2}^2) \right]. \quad (4.44)$$

При произвольных значениях N_1 и $N_{test.1}$ получим

$$m_{13.n} = \sum_{k=1}^{N_1} P_{11.1}^{k-1} \rightarrow$$

$$\leftarrow \cdot \left[1 + P_{12.1} \left[\sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1} + Q_{23.1}^{N_{test.1}} [1 + P_{12.2} (1 + Q_{23.2})] (1 + P_{11.2} + P_{11.2}^2) \right] \right] \rightarrow \quad (4.45)$$

$$\leftarrow + P_{11.1}^{N_1} [1 + P_{12.2} (1 + Q_{23.2})] (1 + P_{11.2} + P_{11.2}^2);$$

$$m_{13.d} = 1 - \left[P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1} \right] \rightarrow$$

$$\leftarrow \cdot \left[P_{11.2}^3 + P_{12.2} Q_{23.2}^2 (1 + P_{11.2} + P_{11.2}^2) \right]. \quad (4.46)$$

Случай 9. Для $N_{FOL} = 2$, $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 3$ и $N_{test.2} = 3$ среднее число шагов для перехода из состояния $a_{1.1.1}$ в состояние успешной синхронизации a_3 равно $m_{13} = m_{13.n}/m_{13.d}$,

$$m_{13.n} = (1 + P_{11.1} + P_{11.1}^2) [1 + P_{12.1} (1 + Q_{23.1} + Q_{23.1}^2)] \rightarrow$$

$$\leftarrow + [P_{11.1}^3 + P_{12.1} Q_{23.1}^3 (1 + P_{11.1} + P_{11.1}^2)] \rightarrow \quad (4.47)$$

$$\leftarrow \cdot (1 + P_{11.2} + P_{11.2}^2) [1 + P_{12.2} (1 + Q_{23.2} + Q_{23.2}^2)];$$

$$m_{13.d} = 1 - [P_{11.1}^3 + P_{12.1} Q_{23.1}^3 (1 + P_{11.1} + P_{11.1}^2)] \rightarrow$$

$$\leftarrow \cdot [P_{11.2}^3 + P_{12.2} Q_{23.2}^3 (1 + P_{11.2} + P_{11.2}^2)]. \quad (4.48)$$

Дисперсия числа шагов, затрачиваемых на переход процесса из непоглощающего состояния $a_{1.1.1}$ в поглощающее состояние a_3 равна

$$d_{13} = 2 \cdot A_{1.1}^{-1} \cdot m_{1.1} + 2 \cdot A_{1.2}^{-1} \cdot m_{2.1} + 2 \cdot A_{1.3}^{-1} \cdot m_{3.1} + 2 \cdot A_{1.4}^{-1} \cdot m_{4.1} + 2 \cdot A_{1.5}^{-1} \cdot m_{5.1} \rightarrow$$

$$\leftarrow +2 \cdot A_{1,6}^{-1} \cdot m_{6,1} + 2 \cdot A_{1,7}^{-1} \cdot m_{7,1} + 2 \cdot A_{1,8}^{-1} \cdot m_{8,1} + 2 \cdot A_{1,9}^{-1} \cdot m_{9,1} + 2 \cdot A_{1,10}^{-1} \cdot m_{10,1} \rightarrow$$

$$\leftarrow +2 \cdot A_{1,11}^{-1} \cdot m_{11,1} + 2 \cdot A_{1,12}^{-1} \cdot m_{12,1} - m_{1,1}^2 - m_{1,1},$$

где $A_{l,n}^{-1}$ – элемент обратной матрицы, находящийся на пересечении l -й строки и n -го столбца (см. формулу (4.6)), $m_{l,n}$ – среднее число шагов для перехода в состояние успешной синхронизации (см. формулу (4.12)).

При произвольных значениях N_1 и $N_{test.1}$

$$m_{13,n} = \sum_{k=1}^{N_1} P_{11.1}^{k-1} [1 + P_{12.1} \sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1}] \rightarrow$$

$$\leftarrow + [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] \rightarrow \quad (4.49)$$

$$\leftarrow \cdot (1 + P_{11.2} + P_{11.2}^2) [1 + P_{12.2} (1 + Q_{23.2} + Q_{23.2}^2)];$$

$$m_{13,d} = 1 - [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] \rightarrow$$

$$\leftarrow \cdot [P_{11.2}^3 + P_{12.2} Q_{23.2}^3 (1 + P_{11.2} + P_{11.2}^2)]. \quad (4.50)$$

Таким образом, для случаев 3, 6 и 9, получим обобщенное выражение для расчёта среднего числа шагов для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 при произвольном количестве тестов $N_{test.1}, N_{test.2}$ и произвольном количестве кадров N_1, N_2 (количество участков в ВОЛС $N_{FOL} = 2$)

$$m_{13,n} = [1 + P_{12.1} \sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1}] \sum_{k=1}^{N_1} P_{11.1}^{k-1} \rightarrow$$

$$\leftarrow + [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] [1 + P_{12.2} \sum_{k=1}^{N_{test.2}} Q_{23.2}^{k-1}] \sum_{k=1}^{N_2} P_{11.2}^{k-1}; \quad (4.51)$$

$$m_{13,d} = 1 - [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] \rightarrow$$

$$\leftarrow \cdot [P_{11.2}^{N_2} + P_{12.2} Q_{23.2}^{N_{test.2}} \sum_{k=1}^{N_2} P_{11.2}^{k-1}]. \quad (4.52)$$

Случай 10. Пусть ВОЛС состоит из трёх участков $N_{FOL} = 3$. Допустимые количество кадров и тестов в участках равны $N_1 = 3$ и $N_{test.1} = 3$, $N_2 = 3$ и $N_{test.2} = 3$, $N_3 = 3$ и $N_{test.3} = 3$. Диаграмму состояний и переходов представим в табличном виде:

	$a_{1.1.1}$	$a_{1.1.2}$	$a_{1.1.3}$	$a_{2.1.1}$	$a_{2.1.2}$	$a_{2.1.3}$	$a_{1.2.1}$	$a_{1.2.2}$	$a_{1.2.3}$	$a_{2.2.1}$	$a_{2.2.2}$	$a_{2.2.3}$	$a_{1.3.1}$	$a_{1.3.2}$	$a_{1.3.3}$	$a_{2.3.1}$	$a_{2.3.2}$	$a_{2.3.3}$	a_3
$a_{1.1.1}$		$P_{11.1}$		$P_{12.1}$															
$a_{1.1.2}$			$P_{11.1}$	$P_{12.1}$															
$a_{1.1.3}$				$P_{12.1}$			$P_{11.1}$												
$a_{2.1.1}$					$Q_{23.1}$														$P_{23.1}$
$a_{2.1.2}$						$Q_{23.1}$													$P_{23.1}$
$a_{2.1.3}$							$Q_{23.1}$												$P_{23.1}$
$a_{1.2.1}$								$P_{11.2}$		$P_{12.2}$									
$a_{1.2.2}$									$P_{11.2}$	$P_{12.2}$									

$a_{1.2.3}$										$P_{12.2}$			$P_{11.2}$						
$a_{2.2.1}$											$Q_{23.2}$								$P_{23.2}$
$a_{2.2.2}$											$Q_{23.2}$								$P_{23.2}$
$a_{2.2.3}$											$Q_{23.2}$								$P_{23.2}$
$a_{1.3.1}$													$P_{11.3}$		$P_{12.3}$				
$a_{1.3.2}$														$P_{11.3}$	$P_{12.3}$				
$a_{1.3.3}$	$P_{11.3}$														$P_{12.3}$				
$a_{2.3.1}$																$Q_{23.3}$			$P_{23.3}$
$a_{2.3.2}$																	$Q_{23.3}$		$P_{23.3}$
$a_{2.3.3}$	$Q_{23.3}$																		$P_{23.3}$
a_3																			

Среднее число шагов для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 равно $m_{13} = m_{13.n}/m_{13.d}$,

$$\begin{aligned}
m_{13.n} &= (1 + P_{11.1} + P_{11.1}^2)[1 + P_{12.1}(1 + Q_{23.1} + Q_{23.1}^2)] \rightarrow \\
&\leftarrow + [P_{11.1}^3 + P_{12.1}Q_{23.1}^3(1 + P_{11.1} + P_{11.1}^2)] \rightarrow \\
&\leftarrow \cdot (1 + P_{11.2} + P_{11.2}^2)[1 + P_{12.2}(1 + Q_{23.2} + Q_{23.2}^2)] \rightarrow \\
&\leftarrow + [P_{11.1}^3 + P_{12.1}Q_{23.1}^3(1 + P_{11.1} + P_{11.1}^2)][P_{11.2}^3 + P_{12.2}Q_{23.2}^3(1 + P_{11.2} + P_{11.2}^2)] \rightarrow \\
&\leftarrow \cdot (1 + P_{11.3} + P_{11.3}^2) \cdot [1 + P_{12.3}(1 + Q_{23.3} + Q_{23.3}^2)];
\end{aligned} \tag{4.53}$$

$$\begin{aligned}
m_{13.d} &= 1 - [P_{11.1}^3 + P_{12.1}Q_{23.1}^3(1 + P_{11.1} + P_{11.1}^2)] \rightarrow \\
&\leftarrow \cdot [P_{11.2}^3 + P_{12.2}Q_{23.2}^3(1 + P_{11.2} + P_{11.2}^2)] \rightarrow \\
&\leftarrow \cdot [P_{11.3}^3 + P_{12.3}Q_{23.3}^3(1 + P_{11.3} + P_{11.3}^2)].
\end{aligned} \tag{4.54}$$

Дисперсия числа шагов, затрачиваемых на переход процесса из непоглощающего состояния $a_{1.1.1}$ в поглощающее состояние a_3 равна

$$\begin{aligned}
d_{13} &= 2 \cdot A_{1,1}^{-1} \cdot m_{1,1} + 2 \cdot A_{1,2}^{-1} \cdot m_{2,1} + 2 \cdot A_{1,3}^{-1} \cdot m_{3,1} + 2 \cdot A_{1,4}^{-1} \cdot m_{4,1} + 2 \cdot A_{1,5}^{-1} \cdot m_{5,1} \rightarrow \\
&\leftarrow + 2 \cdot A_{1,6}^{-1} \cdot m_{6,1} + 2 \cdot A_{1,7}^{-1} \cdot m_{7,1} + 2 \cdot A_{1,8}^{-1} \cdot m_{8,1} + 2 \cdot A_{1,9}^{-1} \cdot m_{9,1} + 2 \cdot A_{1,10}^{-1} \cdot m_{10,1} \rightarrow \\
&\leftarrow + 2 \cdot A_{1,11}^{-1} \cdot m_{11,1} + 2 \cdot A_{1,12}^{-1} \cdot m_{12,1} + 2 \cdot A_{1,13}^{-1} \cdot m_{13,1} + 2 \cdot A_{1,14}^{-1} \cdot m_{14,1} + 2 \cdot A_{1,15}^{-1} \cdot m_{15,1} \rightarrow \\
&\leftarrow + 2 \cdot A_{1,16}^{-1} \cdot m_{16,1} + 2 \cdot A_{1,17}^{-1} \cdot m_{17,1} + 2 \cdot A_{1,18}^{-1} \cdot m_{18,1} - m_{1,1}^2 - m_{1,1},
\end{aligned}$$

где $A_{l,n}^{-1}$ – элемент обратной матрицы, находящийся на пересечении l -й строки и n -го столбца (см. формулу (4.6)), $t_{l,n}$ – среднее число шагов для перехода в состояние успешной синхронизации (см. формулу (4.12)). Отметим, переменная n количественно равна сумме кадров и тестов всех участков ВОЛС $n = \sum_{j=1}^{N_{FOL}} (N_j + N_{test.j})$.

При $N_{FOL} = 3$ и произвольных значениях N_1, N_2, N_3 и $N_{test.1}, N_{test.2}, N_{test.3}$ получим

$$\begin{aligned}
m_{13.n} &= [1 + P_{12.1} \sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1}] \sum_{k=1}^{N_1} P_{11.1}^{k-1} \rightarrow \\
&\leftarrow + [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] [1 + P_{12.2} \sum_{k=1}^{N_{test.2}} Q_{23.2}^{k-1}] \sum_{k=1}^{N_2} P_{11.2}^{k-1} \rightarrow (4.55) \\
&\leftarrow + [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] [P_{11.2}^{N_2} + P_{12.2} Q_{23.2}^{N_{test.2}} \sum_{k=1}^{N_2} P_{11.2}^{k-1}] \rightarrow
\end{aligned}$$

$$\begin{aligned}
&\leftarrow \cdot [1 + P_{12.3} \sum_{k=1}^{N_{test.3}} Q_{23.3}^{k-1}] \sum_{k=1}^{N_3} P_{11.3}^{k-1} ; \\
m_{13.d} &= 1 - [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] \rightarrow \\
&\leftarrow \cdot [P_{11.2}^{N_2} + P_{12.2} Q_{23.2}^{N_{test.2}} \sum_{k=1}^{N_2} P_{11.2}^{k-1}] \rightarrow (4.56) \\
&\leftarrow \cdot [P_{11.3}^{N_3} + P_{12.3} Q_{23.3}^{N_{test.3}} \sum_{k=1}^{N_3} P_{11.3}^{k-1}].
\end{aligned}$$

Таким образом, для случаев 9 и 10, получим обобщенное выражение для расчёта среднего числа шагов и дисперсии для перехода из состояния начала синхронизации $a_{1.1.1}$ в состояние успешной синхронизации a_3 при произвольном количестве тестов $N_{test,j}$, кадров N_j и участков N_{FOL}

$$\begin{aligned}
m_{13.n} &= [1 + P_{12.1} \sum_{k=1}^{N_{test.1}} Q_{23.1}^{k-1}] \sum_{k=1}^{N_1} P_{11.1}^{k-1} \rightarrow \\
&\leftarrow + [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] [1 + P_{12.2} \sum_{k=1}^{N_{test.2}} Q_{23.2}^{k-1}] \sum_{k=1}^{N_2} P_{11.2}^{k-1} \rightarrow \\
&\leftarrow + [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] [P_{11.2}^{N_2} + P_{12.2} Q_{23.2}^{N_{test.2}} \sum_{k=1}^{N_2} P_{11.2}^{k-1}] \rightarrow \\
&\leftarrow \cdot [1 + P_{12.3} \sum_{k=1}^{N_{test.3}} Q_{23.3}^{k-1}] \sum_{k=1}^{N_3} P_{11.3}^{k-1} + \dots + [P_{11.1}^{N_1} + P_{12.1} Q_{23.1}^{N_{test.1}} \sum_{k=1}^{N_1} P_{11.1}^{k-1}] \rightarrow \\
&\leftarrow \cdot [P_{11.2}^{N_2} + P_{12.2} Q_{23.2}^{N_{test.2}} \sum_{k=1}^{N_2} P_{11.2}^{k-1}] \cdot \dots \rightarrow (4.57)
\end{aligned}$$

$$\begin{aligned}
&\leftarrow \cdot [P_{11.(j-1)}^{N_{(j-1)}} + P_{12.(j-1)} Q_{23.(j-1)}^{N_{test.(j-1)}} \sum_{k=1}^{N_{(j-1)}} P_{11.(j-1)}^{k-1}] \rightarrow \\
&\leftarrow \cdot [1 + P_{12.j} \sum_{k=1}^{N_{test.j}} Q_{23.j}^{k-1}] \sum_{k=1}^{N_j} P_{11.j}^{k-1} ; \\
m_{13.d} &= 1 - \prod_{j=1}^{N_{FOL}} [P_{11.j}^{N_j} + P_{12.j} Q_{23.j}^{N_{test.j}} \sum_{k=1}^{N_j} P_{11.j}^{k-1}]. (4.58)
\end{aligned}$$

$$d_{13} = -(m_{1.1}^2 + m_{1.1}) + 2 \cdot \sum_{i=1}^{\sum_{j=1}^{N_{FOL}} (N_j + N_{test.j})} A_{1,i}^{-1} \cdot m_{i,1}.$$

Введём обозначения

$$a_j = [1 + P_{12.j} \sum_{k=1}^{N_{test.j}} Q_{23.j}^{k-1}] \sum_{k=1}^{N_j} P_{11.j}^{k-1} ; (4.59)$$

$$b_j = [P_{11.j}^{N_j} + P_{12.j} Q_{23.j}^{N_{test.j}} \sum_{k=1}^{N_j} P_{11.j}^{k-1}] (4.60)$$

находим

$$m_{13.n} = a_1 + [b_1 \cdot a_2] + [b_1 \cdot b_2 \cdot a_3] + \dots + [b_1 \cdot b_2 \cdot \dots \cdot b_{(j-1)} \cdot a_j] ; (4.61)$$

$$m_{13.d} = 1 - \prod_{j=1}^{N_{FOL}} b_j ; (4.62)$$

$$m_{13} = \frac{a_1 + [b_1 \cdot a_2] + [b_1 \cdot b_2 \cdot a_3] + \dots + [b_1 \cdot b_2 \cdot \dots \cdot b_{(j-1)} \cdot a_j]}{1 - \prod_{j=1}^{N_{FOL}} b_j}. (4.63)$$

Пусть частота генерации ИТГ равна $\xi_{DCR} = 6$ Гц. При обеспечении допустимых вероятностей ошибки синхронизации $P_{err.0}=0,01; 0,02; 0,05$ и $0,10$ протяжённость ВОЛС составляет 33,4; 46,4; 65,9 и 82 км соответственно (см. таблицу 3.1), причём период следования синхроимпульсов равен 83,33; 166,67; 500 и 1000 мкс. В ОВ Corning® SMF-28 $\alpha_{OF} = 0,18$ дБ/км и $n_{OF} = 1,4682$. Длительность синхроимпульса $\tau_s=300$ пс. Нестабильность периода следования импульсов ΔT_s и временное отклонение момента прихода фотона вследствие наличия в ОВ дисперсионных свойств τ_{OF} отсутствуют.

Результаты расчёта среднего времени синхронизации при различных значениях допустимой вероятности ошибки синхронизации $P_{err.0}$ представлены в таблице 4.1.

Таблица 4.1 – Результаты расчёта вероятностных и временных характеристик алгоритма синхронизации графоаналитическим методом

$P_{err.0}$	Параметр	Участок ВОЛС, j									
		1	2	3	4	5	6	7	8	9	10
0,01	$P_{11.j}$	0,9247	0,9381	0,9476	0,9546	0,9600	0,9643	0,9678	0,9706	0,9730	0,9751
	$P_{12.j}$	0,0753	0,0619	0,0524	0,0454	0,0400	0,0357	0,0322	0,0294	0,0270	0,0249
	$Q_{23.j}$	0,9250	0,9384	0,9478	0,9548	0,9602	0,9645	0,9679	0,9708	0,9732	0,9752
	m_{13}	26,6530									
	T_s , МКС	83,33									
	$\bar{\tau}_{sync}$, мс	2,22									
0,02	$P_{11.j}$	0,9359	0,9526	0,9626	0,9692	0,9739	0,9774	0,9801	0,9822	0,9840	0,9854
	$P_{12.j}$	0,0641	0,0474	0,0374	0,0308	0,0261	0,0226	0,0199	0,0178	0,0160	0,0146
	$Q_{23.j}$	0,9365	0,9530	0,9629	0,9695	0,9742	0,9776	0,9803	0,9824	0,9841	0,9855
	m_{13}	31,5061									
	T_s , МКС	166,67									
	$\bar{\tau}_{sync}$, мс	5,25									
0,05	$P_{11.j}$	0,9534	0,9707	0,9790	0,9838	0,9869	0,9890	0,9905	0,9917	0,9926	0,9934
	$P_{12.j}$	0,0466	0,0293	0,0210	0,0162	0,0131	0,0110	0,0095	0,0083	0,0074	0,0066
	$Q_{23.j}$	0,9544	0,9714	0,9795	0,9842	0,9872	0,9892	0,9907	0,9919	0,9928	0,9935
	m_{13}	44,2165									
	T_s , МКС	500,00									
	$\bar{\tau}_{sync}$, мс	22,11									
0,10	$P_{11.j}$	0,9660	0,9813	0,9875	0,9907	0,9927	0,9940	0,9949	0,9956	0,9961	0,9965
	$P_{12.j}$	0,0340	0,0187	0,0125	0,0093	0,0073	0,0060	0,0051	0,0044	0,0039	0,0035
	$Q_{23.j}$	0,9675	0,9821	0,9880	0,9911	0,9930	0,9942	0,9951	0,9958	0,9963	0,9967
	m_{13}	63,4672									
	T_s , МКС	1000,00									
	$\bar{\tau}_{sync}$, мс	63,47									

Среднее время синхронизации при $P_{err.0}=0,10$ составляет 63,47 мс. Ужесточение требований к вероятности ошибки синхронизации в 10 раз (с 0,10 до 0,01) приводит к сокращению длины ВОЛС почти в 2,5 раза (82 км против 33,4 км) и среднего времени синхронизации в 28,6 раза (63,47 мс против 2,22 мс).

Отклонение результатов расчёта среднего времени синхронизации графоаналитическим методом от результатов моделирования (см. таблицу 3.12) составляет 2,8; 2,1; 2,0 и 1,4 % при $P_{err.0}=0,01; 0,02; 0,05$ и $0,10$ соответственно. Незначительное отклонение указывает на возможность использовать полученные аналитические выражения для расчёта среднего времени синхронизации станций системы КРК согласно предложенному алгоритму.

Однако, в связи с большим количеством кадров, допустимых на этапе поиска, и большим количеством тестов, допустимых на этапе тестирования, рассмотренный графоаналитический метод становится вычислительно сложной задачей для расчёта дисперсии времени синхронизации даже в случае, когда ВОЛС состоит всего из 2-х участков. Учитывая достоверность полученных аналитических выражений для расчёта среднего времени синхронизации, подтверждённую сравнительным анализом теоретических расчётов и моделирования, будем считать полученные при моделировании результаты дисперсии и СКО также достоверными.

Указанные результаты получены при определённых ограничениях на количество кадров N_j и тестов $N_{test.j}$ для каждого участка ВОЛС. Рассчитаем среднее время синхронизации при отсутствии указанных ограничений.

Допустим, максимальное количество кадров и тестов для участка не ограничено $N_j \rightarrow \infty, N_{test.j} \rightarrow \infty$. Следовательно, будут выполняться условия

$$\begin{aligned} a_j < a_{j,max} &= \left[1 + P_{12.j} \sum_{k=1}^{\infty} Q_{23.j}^{k-1} \right] \sum_{k=1}^{\infty} P_{11.j}^{k-1} \\ &= \left[1 + \frac{P_{12.j}}{Q_{23.j}} \sum_{k=1}^{\infty} Q_{23.j}^k \right] \frac{1}{P_{11.j}} \sum_{k=1}^{\infty} P_{11.j}^k ; \\ b_j < b_{j,max} &= \left[P_{11.j}^{N_j} + P_{12.j} Q_{23.j}^{N_{test.j}} \sum_{k=1}^{\infty} P_{11.j}^{k-1} \right] \\ &= \left[P_{11.j}^{N_j} + \frac{P_{12.j} Q_{23.j}^{N_{test.j}}}{P_{11.j}} \sum_{k=1}^{\infty} P_{11.j}^k \right]. \end{aligned}$$

Согласно формуле (5.2.2.1) [110]

$$\sum_{k=1}^{\infty} P_{11.j}^k = \frac{P_{11.j}}{1 - P_{11.j}} ; \sum_{k=1}^{\infty} Q_{23.j}^k = \frac{Q_{23.j}}{1 - Q_{23.j}} .$$

Тогда

$$a_{j.max} = \frac{\frac{P_{12.j}}{Q_{23.j} - 1} - 1}{P_{11.j} - 1} = \frac{P_{12.j} - Q_{23.j} + 1}{(P_{11.j} - 1)(Q_{23.j} - 1)} ;$$

$$b_{j.max} = P_{11.j}^{N_j} - \frac{P_{12.j} Q_{23.j}^{N_{test.j}}}{P_{11.j} - 1} .$$

Следовательно

$$m_{13} = \frac{a_{1.max} + [b_{1.max} \cdot a_{2.max}] + \dots + [b_{1.max} \cdot b_{2.max} \cdot \dots \cdot b_{(j-1).max} \cdot a_{j.max}]}{1 - \prod_{j=1}^{N_{FOL}} b_{j.max}} .$$

Результаты расчёта среднего времени синхронизации при различных значениях допустимой вероятности ошибки синхронизации $P_{err.0}$ при неограниченном количестве кадров и тестов представлены в таблице 4.2.

Как и следовало ожидать, при неограниченном количестве кадров и тестов $N_j \rightarrow \infty$, $N_{test.j} \rightarrow \infty$ среднее время синхронизации больше $\overline{\tau_{sync.max}} > \overline{\tau_{sync}}$, по сравнению со средним временем синхронизации с ограничениями по количеству кадров и тестов. Так, отклонение среднего времени синхронизации $\overline{\tau_{sync}}$ от среднего времени синхронизации при неограниченном количестве кадров и тестов $\overline{\tau_{sync.max}}$ составляет 0,50; 1,02; 2,63 и 5,47 % при обеспечении допустимых вероятностей ошибки синхронизации на уровне $P_{err.0}=0,01$; 0,02; 0,05 и 0,10 соответственно. Полученные аналитические выражения для расчёта среднего времени синхронизации $\overline{\tau_{sync.max}}$ значительно проще полученных графоаналитическим методом выражений. В связи с незначительным отклонением полученных результатов (не более 5,47 % для среднего времени синхронизации) полученные аналитические выражения могут быть использованы для экспресс-расчёта среднего времени синхронизации графоаналитическим методом.

Таблица 4.2 – Результаты расчёта вероятностных и временных характеристик алгоритма синхронизации графоаналитическим методом при неограниченном количестве кадров и тестов

$P_{err.0}$	Параметр	Участок ВОЛС, j									
		1	2	3	4	5	6	7	8	9	10
0,01	T_s , мкс	83,33									
	$a_{j,max}$	26,61	32,37	38,23	44,14	50,13	56,16	62,19	68,25	74,34	80,49
	$\frac{a_j - a_{j,max}}{a_j}$, %	0,50	0,49	0,49	0,49	0,49	0,50	0,50	0,49	0,50	0,49
	$b_{j,max} \cdot 10^{-3}$	5,5	5,3	5,3	5,3	5,4	5,4	5,5	5,4	5,5	5,4
	$\frac{b_j - b_{j,max}}{b_j}$, %	0,08	0,08	0,08	0,08	0,08	0,08	0,08	0,08	0,08	0,08
	$m_{13,max}$	26,7866									
	$\frac{m_{13} - m_{13,max}}{m_{13}}$, %	0,50									
	$\tau_{sync,max}$, мс	2,23									
0,02	T_s , мкс	166,67									
	$a_{j,max}$	31,35	42,36	53,70	65,30	77,12	88,99	100,94	113,08	125,30	137,48
	$\frac{a_j - a_{j,max}}{a_j}$, %	1,02	1,00	0,99	1,00	1,00	1,01	1,02	1,01	1,02	1,01
	$b_{j,max} \cdot 10^{-3}$	11,0	10,9	10,8	10,9	10,9	11,0	11,1	11,0	11,1	11,0
	$\frac{b_j - b_{j,max}}{b_j}$, %	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16
	$m_{13,max}$	31,8270									
	$\frac{m_{13} - m_{13,max}}{m_{13}}$, %	1,02									
	$\tau_{sync,max}$, мс	5,30									
0,05	T_s , мкс	500,00									
	$a_{j,max}$	43,37	69,06	96,47	124,90	154,05	183,55	213,56	243,83	274,45	305,06
	$\frac{a_j - a_{j,max}}{a_j}$, %	2,61	2,60	2,61	2,61	2,62	2,62	2,62	2,61	2,61	2,61
	$b_{j,max} \cdot 10^{-3}$	27,9	27,8	28,0	28,0	28,1	28,0	28,0	27,9	28,0	28,0
	$\frac{b_j - b_{j,max}}{b_j}$, %	0,40	0,41	0,41	0,41	0,41	0,41	0,41	0,41	0,41	0,41
	$m_{13,max}$	45,3776									
	$\frac{m_{13} - m_{13,max}}{m_{13}}$, %	2,63									
	$\tau_{sync,max}$, мс	22,69									
0,10	T_s , мкс	1000,00									
	$a_{j,max}$	60,25	109,46	163,52	220,26	278,91	338,60	399,12	460,54	522,45	584,92
	$\frac{a_j - a_{j,max}}{a_j}$, %	5,37	5,46	5,52	5,49	5,51	5,54	5,54	5,52	5,52	5,52
	$b_{j,max} \cdot 10^{-3}$	56,0	56,9	57,4	57,1	57,3	57,6	57,6	57,4	57,5	57,5
	$\frac{b_j - b_{j,max}}{b_j}$, %	0,82	0,83	0,83	0,83	0,83	0,83	0,83	0,83	0,83	0,83
	$m_{13,max}$	66,9396									
	$\frac{m_{13} - m_{13,max}}{m_{13}}$, %	5,47									
	$\tau_{sync,max}$, мс	66,94									
	$\frac{\tau_{sync} - \tau_{sync,max}}{\tau_{sync}}$, %	5,47									

Резюме. Получены аналитические выражения для расчёта среднего и дисперсии времени синхронизации станций предлагаемого алгоритма синхронизации графоаналитическим методом в общем случае при произвольном

количестве участков, кадров и тестов. Ужесточение требований к вероятности ошибки синхронизации на порядок позволяет сократить среднее время синхронизации в десятки раз (в 28,6 раза). Достоверность полученных аналитических выражений для расчёта среднего времени синхронизации подтверждается незначительным отклонением от результатов моделирования (не более 2,8 %). Получены аналитические выражения для экспресс-расчёта среднего времени синхронизации, причём отклонение при экспресс-расчёте составляет не более 5,47 %. Отмечена вычислительная сложность применения графоаналитического метода для расчёта дисперсии времени синхронизации станций системы КРК.

4.4 Определение статистических характеристик этапа тестирования в шумовом участке ВОЛС

Проведём расчёт среднего и дисперсии времени тестирования в двухэтапном алгоритме синхронизации при допущении, что анализируемый участок ВОЛС является шумовым.

Этап тестирования в предлагаемом двухэтапном алгоритме синхронизации идентичен от участка к участку, изменяется только максимальное допустимое количество тестов $N_{test,j}$. На рисунке 4.2 представлен этап тестирования с вероятностями переходов между состояниями.

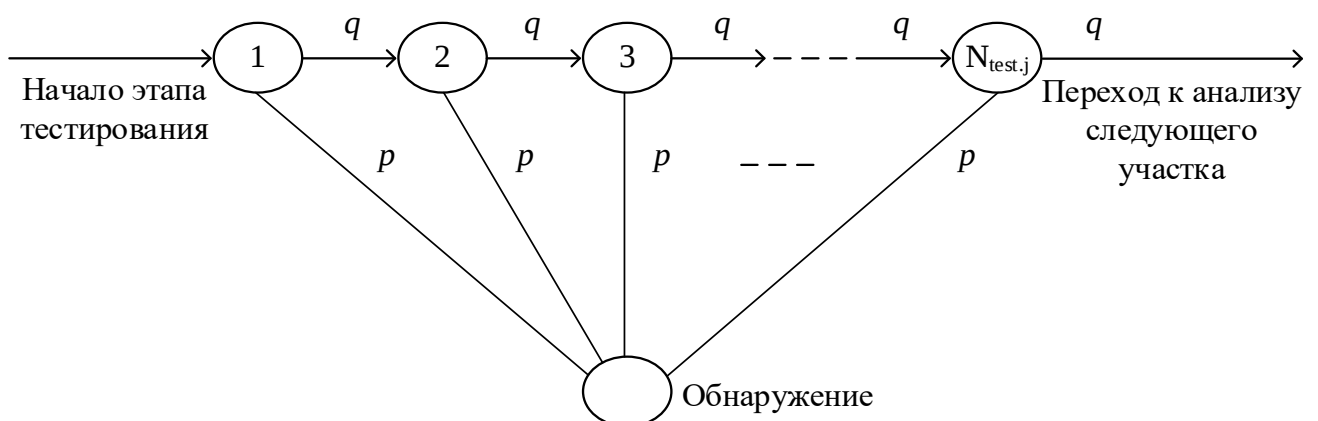


Рисунок 4.2 – Диаграмма состояний и переходов этапа тестирования

Пусть $p_{kj} = p_j, k = \overline{1, N_{test,j}}$ – вероятность срабатывания аппаратуры (обнаружения фотона или ИТТ) во время k_j -го теста в j -м участке; $q_{kj} = q_j, k_j =$

$\overline{1, N_{test.j}}$ – вероятность отсутствия срабатывания аппаратуры (обнаружения фотона или ИТТ) во время k_j -го теста. Причём $q_{kj} = 1 - p_{kj}$ и $q_j = 1 - p_j$.

Проанализируем случай ложного срабатывания на этапе поиска. Тогда вероятности p_0 и q_0 определяются только средним числом ИТТ за длительность теста (импульса стробирования), которое равно $\overline{n_{DCR.strob}} = \xi_{DCR} \cdot \tau_{strob}$ и фиксировано для всех тестов. Причём $q_0 = q_j = 1 - \overline{n_{DCR.strob}} = 1 - \xi_{DCR} \cdot \tau_{strob}$ и $p_0 = p_j = \overline{n_{DCR.strob}}$.

Для обнаружения ложного срабатывания на этапе поиска потребуется время

$$\tau_{00} = N_{test.j} \cdot q_0^{N_{test.j}} \cdot T_s = N_{test.j} \cdot (1 - \overline{n_{DCR.strob}})^{N_{test.j}} \cdot T_s.$$

Применив бином Ньютона и ограничившись первыми двумя слагаемыми, находим

$$\tau_{00} \cong N_{test.j} \cdot q_0^{N_{test.j}} \cdot T_s = N_{test.j} \cdot (1 - N_{test.j} \cdot \overline{n_{DCR.strob}}) \cdot T_s.$$

Важно, время на обнаружение ложного срабатывания на этапе поиска фиксировано.

Выборочное среднее время (несмещённая оценка) на принятие ложного решения на этапе тестирования для анализируемого случая определяется формулой

$$\overline{\tau_{01}} = \sum_{k_j=1}^{N_{test.j}} q_0^{k_j-1} p_0 k_j T_s.$$

Здесь вероятность ложного срабатывания во время теста равна

$$p_0 = p_{test0} = 1 - \exp(-\overline{n_{strob}}) \cong \overline{n_{DCR.strob}} = \xi_{DCR} \cdot \tau_{strob},$$

а вероятность принятия правильного решения об отсутствии фотона

$$q_0 = 1 - p_0 \cong 1 - \xi_{DCR} \cdot \tau_{strob}.$$

Формула для вычисления смещённой оценки дисперсии времени на принятие ложного решения на этапе тестирования по последовательности реализаций величины $\tau_{01} = T_s, 2T_s, 3T_s, \dots, N_{test.j}T_s$, имеет вид

$$\overline{\sigma_{\tau_{01}}}^2 = \frac{1}{N_{test.j}} \cdot \sum_{k_j=1}^{N_{test.j}} q_0^{k_j-1} p_0 (k_j T_s - \overline{\tau_{01}})^2.$$

Несмещённая оценка дисперсии случайного времени на принятие ложного решение на этапе тестирования равна

$$\widetilde{\sigma_{\tau_{01}}}^2 = \frac{1}{N_{test.j} - 1} \cdot \sum_{k_j=1}^{N_{test.j}} q_0^{k_j-1} p_0 (k_j T_s - \overline{\tau_{01}})^2.$$

Пусть частота генерации ИТТ $\xi_{DCR} = 6$ Гц. При обеспечении допустимых вероятностей ошибки синхронизации $P_{err.0} = 0,01; 0,02; 0,05$ и $0,10$ протяжённость ВОЛС составляет 33,4; 46,4; 65,9 и 82 км соответственно (см. таблицу 3.1), причём период следования синхроимпульсов равен 83,33; 166,67; 500 и 1000 мкс. Для ОВ Corning® SMF-28 $\alpha_{OF} = 0,18$ дБ/км и $n_{OF} = 1,4682$. Длительность синхроимпульса $\tau_s = 300$ пс. Нестабильность периода следования импульсов ΔT_s и временное отклонение момента прихода фотона из-за дисперсии в ОВ τ_{OF} отсутствуют.

Результаты расчёта среднего и дисперсии времени тестирования с принятием ложного решения на этапе тестирования при различных допустимых вероятностях ошибки синхронизации $P_{err.0}$ представлены в таблице 4.3.

Среднее время тестирования в j -м шумовом участке определяется суммой затраченного времени на принятие правильного решения о ложном срабатывании на этапе поиска τ_{00} и выборочного среднего времени (несмещённая оценка) на принятие ложного решения на этапе тестирования для анализируемого случая $\overline{\tau_{01}}$. Причём выборочное среднее время $\overline{\tau_{01}}$ составляет не более трёхтысячной процента от предельного времени на тестирование при изменении допустимой вероятности ошибки синхронизации $P_{err.0}$ в пределах от 0,01 до 0,10. Исходя из полученных результатов, можно принять $\tau_{00} + \overline{\tau_{01}} \cong \tau_{00}$.

Отметим, среднее число тестов, затрачиваемое на этапе тестирования в j -м шумовом участке, определяемое как отношение среднего времени тестирования к периоду следования синхроимпульсов τ_{00}/T_s , близко к предельному числу тестов $N_{test.j}$, допустимых на этапе тестирования. Это обусловлено ложным срабатыванием на этапе поиска и, следовательно, отрицательным результатом тестирования за предельное число тестов. При этом отношение смещённой оценки СКО времени на принятие ложного решения на этапе тестирования и времени на

правильное решение о ложном срабатывании на этапе поиска $\overline{\sigma_{\tau_{01}}}/\tau_{00}$ не превышает 0,004%. Таким образом, среднее время тестирования в j-м шумовом участке с учётом СКО равно $\tau_{00} \pm 3\overline{\sigma_{\tau_{01}}}$. Вследствие достаточно низкой вероятности повторного ложного срабатывания на этапе тестирования в шумовом участке увеличением результирующего среднего времени тестирования можно пренебречь.

Таблица 4.3 – Среднее и дисперсия времени тестирования в j-м шумовом участке

$P_{err.0}$	Параметр	Участок ВОЛС, j									
		1	2	3	4	5	6	7	8	9	10
0,01	T_s , мкс	83,33									
	τ_{strob} , пс	600									
	$N_{test.j}$	89	109	129	150	171	191	212	233	254	276
	τ_{00} , мс	7,4	9,1	10,7	12,5	14,2	15,9	17,7	19,4	21,2	23,0
	$\overline{\tau_{01}}$, нс	1,2	1,8	2,5	3,4	4,4	5,5	6,8	8,2	9,7	11,5
	$\overline{\sigma_{\tau_{01}}}^2 \cdot 10^{-14}$	6,7	10,0	14,0	18,9	24,6	30,6	37,7	45,5	54,1	63,8
	$\overline{\sigma_{\tau_{01}}}$, мкс	0,26	0,32	0,37	0,44	0,50	0,55	0,61	0,67	0,74	0,80
0,02	T_s , мкс	166,67									
	τ_{strob} , пс	600									
	$N_{test.j}$	95	130	165	201	238	275	312	350	388	427
	τ_{00} , мс	15,8	21,7	27,5	33,5	39,7	45,8	52,0	58,3	64,7	71,2
	$\overline{\tau_{01}}$, нс	2,7	5,1	8,2	12,2	17,1	22,8	29,3	36,9	45,3	54,8
	$\overline{\sigma_{\tau_{01}}}^2 \cdot 10^{-12}$	0,31	0,57	0,92	1,4	1,9	2,5	3,3	4,1	5,0	6,1
	$\overline{\sigma_{\tau_{01}}}$, мкс	0,55	0,75	0,96	1,2	1,4	1,6	1,8	2,0	2,2	2,5
0,05	T_s , мкс	500									
	τ_{strob} , пс	600									
	$N_{test.j}$	114	183	256	332	411	490	570	651	733	815
	τ_{00} , мс	57,0	91,5	128,0	166,0	205,5	245,0	285,0	325,5	366,5	407,5
	$\overline{\tau_{01}}$, нс	11,8	30,3	59,2	99,5	152,4	216,5	292,9	382,0	484,2	598,5
	$\overline{\sigma_{\tau_{01}}}^2 \cdot 10^{-12}$	4,0	10,1	19,8	33,2	50,9	72,3	97,7	127,4	161,5	199,6
	$\overline{\sigma_{\tau_{01}}}$, мкс	2,0	3,2	4,4	5,8	7,1	8,5	9,9	11,3	12,7	14,1
0,10	T_s , мкс	1000									
	τ_{strob} , пс	600									
	$N_{test.j}$	140	256	383	517	655	796	939	1083	1229	1376
	τ_{00} , мс	140	256	383	517	655	796	939	1083	1229	1376
	$\overline{\tau_{01}}$, нс	35,5	118,4	264,7	482,1	773,4	1142	1589	2113	2721	3411
	$\overline{\sigma_{\tau_{01}}}^2 \cdot 10^{-10}$	0,24	0,79	1,8	3,2	5,2	7,6	10,6	14,1	18,1	22,7
	$\overline{\sigma_{\tau_{01}}}$, мкс	4,9	8,9	13,3	17,9	22,7	27,6	32,6	37,5	42,6	47,7

Резюме. Проведён анализ статистических характеристик этапа тестирования в шумовом участке ВОЛС, получена диаграмма состояний и переходов этапа тестирования. Определены количественно среднее и дисперсия времени тестирования с принятием ложного решения на этапе тестирования при различных значениях допустимой вероятности ошибки синхронизации. Так, среднее число

тестов на этапе тестирования близко к предельному числу тестов, что объясняется отсутствием сигнальных импульсов в анализируемом шумовом участке и, следовательно, гарантирует правильность тестирования при анализе шумового временного интервала.

4.5 Определение статистических характеристик этапа тестирования в сигнальном участке ВОЛС

Проведём расчёт среднего и дисперсии времени тестирования в двухэтапном алгоритме синхронизации при допущении, что анализируемый участок ВОЛС является сигнальным.

Полученные ранее соотношения для расчёта среднего и дисперсии на этапе тестирования в шумовом участке применимы для расчёта временных характеристик для сигнального участка ВОЛС с одной корректировкой – среднее число фотонов и ИТТ за длительность теста (импульса стробирования)

$$\overline{n_{strob}} = \overline{n_{s,j}} + \xi_{DCR} \cdot \tau_{strob} \cong \overline{n_{s,j}} = \overline{n_{s0}} \cdot 10^{-\frac{\alpha_{OF}[\text{дБ/км}] \cdot L_j[\text{км}]}{10}}.$$

Важно, что значение $\overline{n_{s,j}}$, которое рассчитывается по формуле (3.37), зависит от дальности до корреспондента, а, следовательно, и от момента обнаружения сигнальных импульсов в участке $t_{l_{js_1}}$ во время поиска.

Условное выборочное среднее время (несмещённая оценка) для обнаружения на этапе тестирования для анализируемого случая определяется формулой

$$\overline{\tau_{11}(L_j)} = \sum_{k_j=1}^{N_{test,j}} q_1^{k_j-1} p_1 k_j T_s = \frac{p_1}{q_1} T_s \sum_{k_j=1}^{N_{test,j}} k_j q_1^{k_j}.$$

Вероятность правильного решения о приёме фотона во время теста равна

$$p_1 = 1 - \exp(-\overline{n_{strob}}) \cong \overline{n_{s,j}} + \xi_{DCR} \cdot \tau_{strob} \cong \overline{n_{s,j}} = \overline{n_{s0}} \cdot 10^{-\frac{\alpha_{OF}[\text{дБ/км}] \cdot L_j[\text{км}]}{10}},$$

а вероятность пропуска фотона

$$q_1 = 1 - p_1 \cong 1 - \overline{n_{s,j}} = 1 - \overline{n_{s0}} \cdot 10^{-\frac{\alpha_{OF}[\text{дБ/км}] \cdot L_j[\text{км}]}{10}}.$$

Формула для вычисления смещённой оценки дисперсии времени на принятие решения об обнаружении фотона на этапе тестирования по последовательности реализаций случайной величины $\tau_{11} = T_s, 2T_s, 3T_s, \dots, N_{test.j}T_s$, имеет вид

$$\overline{\sigma_{\tau_{11}}}^2 = \frac{1}{N_{test.j}} \cdot \sum_{k_j=1}^{N_{test.j}} q_1^{k_j-1} p_1 (k_j T_s - \overline{\tau_{11}})^2.$$

Несмещённая оценка дисперсии случайного времени на принятие решения об обнаружении на этапе тестирования равна

$$\widetilde{\sigma_{\tau_{11}}}^2 = \frac{1}{N_{test.j} - 1} \cdot \sum_{k_j=1}^{N_{test.j}} q_1^{k_j-1} p_1 (k_j T_s - \overline{\tau_{11}})^2.$$

Результаты расчёта среднего и дисперсии времени тестирования при различных значениях допустимой вероятности ошибки синхронизации $P_{err.0}$ на верхних границах участков представлены в таблице 4.4. Отметим, 0-й участок ВОЛС соответствует нижней границе 1-го участка.

Очевидно, при ухудшении допустимой вероятности ошибки синхронизации в 10 раз (с 0,01 до 0,10), среднее время тестирования значительно возрастает (в 27,1 раза) при тестировании в 1-м участке ВОЛС (28,76 мс против 1,06 мс). При переходе от участка к участку среднее время тестирования также увеличивается. Так, при $P_{err.0}=0,01$ среднее время тестирования в 1-м участке ВОЛС составляет 1,06 мс, во 2-м участке – 1,30 мс, в 10-м участке – 3,30 мс, причём увеличение среднего времени тестирования $\overline{\tau_{11}}$ имеет линейный характер и обусловлено увеличением допустимого количества тестов $N_{test.j}$. СКО не превышает 10,8; 10,4; 9,4 и 8,4 % от значения $\overline{\tau_{11}}$ при $P_{err.0}=0,01; 0,02; 0,05$ и 0,10 соответственно. Отметим, в связи с неидеальностью системы среднее время тестирования в сигнальном участке находится в диапазоне $\overline{\tau_{11}} \pm 3\widetilde{\sigma_{\tau_{11}}}$.

Таблица 4.4 – Среднее и дисперсия времени тестирования на верхних границах участков ВОЛС

$P_{err.0}$	Параметр	Участок ВОЛС, j										
		0	1	2	3	4	5	6	7	8	9	10
0,01	T_s , мкс	83,33										
	τ_{strob} , пс	600										
	$N_{test.j}$	89		109	129	150	171	191	212	233	254	276
	$\overline{\tau_{11}}$, мс	0,83	1,06	1,30	1,54	1,79	2,04	2,29	2,54	2,79	3,04	3,30
	$\widetilde{\sigma_{\tau_{11}}}^2 \cdot 10^{-8}$	0,80	1,31	1,62	1,94	2,26	2,58	2,92	3,25	3,58	3,91	4,24
	$\widetilde{\sigma_{\tau_{11}}}$, мс	0,09	0,114	0,127	0,139	0,150	0,161	0,171	0,180	0,189	0,198	0,206
0,02	T_s , мкс	166,67										
	τ_{strob} , пс	600										
	$N_{test.j}$	95		130	165	201	238	275	312	350	388	427
	$\overline{\tau_{11}}$, мс	1,67	2,51	3,42	4,36	5,31	6,29	7,27	8,25	9,25	10,26	11,27
	$\widetilde{\sigma_{\tau_{11}}}^2 \cdot 10^{-8}$	2,99	6,81	9,38	12,08	14,83	17,61	20,41	23,24	26,10	28,99	31,81
	$\widetilde{\sigma_{\tau_{11}}}$, мс	0,17	0,261	0,306	0,348	0,385	0,420	0,452	0,482	0,511	0,538	0,564
0,05	T_s , мкс	500										
	τ_{strob} , пс	600										
	$N_{test.j}$	114		183	256	332	411	490	570	651	733	815
	$\overline{\tau_{11}}$, мс	5,00	10,42	16,72	23,42	30,38	37,53	44,76	52,10	59,51	67,02	74,51
	$\widetilde{\sigma_{\tau_{11}}}^2 \cdot 10^{-7}$	2,25	9,66	15,68	22,14	28,82	35,62	42,54	49,61	56,72	63,91	71,08
	$\widetilde{\sigma_{\tau_{11}}}$, мс	0,47	0,983	1,252	1,488	1,698	1,887	2,063	2,227	2,381	2,528	2,666
0,10	T_s , мкс	1000										
	τ_{strob} , пс	600										
	$N_{test.j}$	140		256	383	517	655	796	939	1083	1229	1376
	$\overline{\tau_{11}}$, мс	10,00	28,76	52,53	78,62	106,0	134,4	163,2	192,4	222,1	252,0	282,2
	$\widetilde{\sigma_{\tau_{11}}}^2 \cdot 10^{-6}$	0,73	5,86	10,81	16,25	21,95	27,86	33,85	39,93	46,12	52,34	58,63
	$\widetilde{\sigma_{\tau_{11}}}$, мс	0,86	2,421	3,288	4,032	4,686	5,278	5,818	6,319	6,791	7,235	7,657

Указанные результаты получены при ограниченном количестве тестов $N_{test.j}$ для каждого участка. Рассчитаем среднее и дисперсию времени тестирования в сигнальном участке ВОЛС при отсутствии ограничений на количество тестов.

Допустим, максимальное количество тестов для участка не ограничено $N_{test.j} \rightarrow \infty$. Следовательно, будет выполняться условие

$$\overline{\tau_{11}(L_j)} < \overline{\tau_{11.max}(L_j)} = \frac{p_1}{q_1} T_s \sum_{k_j=1}^{\infty} k_j q_1^{k_j}.$$

Согласно [110]

$$\sum_{k_j=1}^{\infty} k_j q_1^{k_j} = \frac{q_1}{(1 - q_1)^2} = \frac{q_1}{p_1^2} \cong \frac{1 - \overline{n_{s,j}}}{\overline{n_{s,j}}^2}.$$

Следовательно, $p_1/q_1 \cong \overline{n_{s,j}}/(1 - \overline{n_{s,j}})$. Тогда

$$\overline{\tau_{11.max}(L_j)} = T_s \cdot \frac{\overline{n_{s,j}}}{1 - \overline{n_{s,j}}} \cdot \frac{1 - \overline{n_{s,j}}}{\overline{n_{s,j}}^2} = \frac{T_s}{\overline{n_{s,j}}}.$$

Несмещённая оценка дисперсии случайного времени на принятие решения об обнаружении на этапе тестирования равна

$$\begin{aligned}\sigma_{\tau_{11.max}}^2 &= \frac{1}{N_{test.j} - 1} \cdot \sum_{k_j=1}^{\infty} q_1^{k_j-1} p_1 (k_j T_s - \overline{\tau_{11.max}})^2 \rightarrow \\ &\leftarrow = \frac{T_s^2}{N_{test.j} - 1} \cdot \frac{p_1}{q_1} \cdot \sum_{k_j=1}^{\infty} \left(k_j^2 q_1^{k_j} - 2 \frac{1}{\overline{n_{s.j}}} k_j q_1^{k_j} + \frac{1}{\overline{n_{s.j}}^2} q_1^{k_j} \right).\end{aligned}$$

Преобразуем выражение под знаком суммы. Согласно [110]

$$\begin{aligned}\sum_{k_j=1}^{\infty} k_j^2 q_1^{k_j} &= \frac{q_1(1+q_1)}{(1-q_1)^3} = \frac{q_1(1+q_1)}{p_1^3}; \\ 2 \frac{1}{\overline{n_{s.j}}} \sum_{k_j=1}^{\infty} k_j q_1^{k_j} &= 2 \frac{1}{\overline{n_{s.j}}} \cdot \frac{q_1}{(1-q_1)^2} = 2 \frac{1}{\overline{n_{s.j}}} \cdot \frac{q_1}{p_1^2}; \\ \frac{1}{\overline{n_{s.j}}^2} \sum_{k_j=1}^{\infty} q_1^{k_j} &= \frac{1}{\overline{n_{s.j}}^2} \cdot \left(\frac{1}{1-q_1} - 1 \right) = \frac{1}{\overline{n_{s.j}}^2} \cdot \frac{q_1}{1-q_1} = \frac{1}{\overline{n_{s.j}}^2} \cdot \frac{q_1}{p_1}.\end{aligned}$$

Тогда

$$\sigma_{\tau_{11.max}}^2 = \frac{T_s^2}{N_{test.j} - 1} \cdot \frac{p_1}{q_1} \cdot \left[\frac{q_1(1+q_1)}{p_1^3} - 2 \frac{1}{\overline{n_{s.j}}} \cdot \frac{q_1}{p_1^2} + \frac{1}{\overline{n_{s.j}}^2} \cdot \frac{q_1}{p_1} \right].$$

Учитывая, что $p_1 \cong \overline{n_{s.j}}$, получим

$$\begin{aligned}\sigma_{\tau_{11.max}}^2 &= \frac{T_s^2}{N_{test.j} - 1} \cdot \frac{p_1}{q_1} \cdot \left[\frac{q_1(1+q_1)}{p_1^3} - 2 \frac{1}{p_1} \cdot \frac{q_1}{p_1^2} + \frac{1}{p_1^2} \cdot \frac{q_1}{p_1} \right] \rightarrow \\ &\leftarrow = \frac{T_s^2}{N_{test.j} - 1} \cdot \frac{q_1}{p_1^2}.\end{aligned}$$

Результаты расчёта среднего $\overline{\tau_{11.max}(L_j)}$ и дисперсии $\sigma_{\tau_{11.max}}^2$ времени тестирования в сигнальном участке представлены в таблице 4.5.

Таблица 4.5 – Среднее и дисперсия времени тестирования на верхних границах участков ВОЛС

$P_{err.0}$	Параметр	Участок ВОЛС, j									
		1	2	3	4	5	6	7	8	9	10
0,01	T_s , мкс	83,33									
	τ_{strob} , пс	600									
	$N_{test.j}$	89	109	129	150	171	191	212	233	254	276
	$\overline{\tau_{11,max}}$, мс	1,07	1,31	1,55	1,80	2,05	2,30	2,56	2,81	3,06	3,32
	$\frac{ \overline{\tau_{11}} - \overline{\tau_{11,max}} }{\overline{\tau_{11}}}$, %	0,58	0,62	0,65	0,66	0,67	0,70	0,71	0,71	0,72	0,72
	$\sigma_{\tau_{11,max}}^2 \cdot 10^{-8}$	1,20	1,49	1,79	2,08	2,37	2,69	2,99	3,30	3,61	3,91
	$\frac{ \sigma_{\tau_{11}}^2 - \sigma_{\tau_{11,max}}^2 }{\sigma_{\tau_{11}}^2}$, %	8,38	8,23	8,08	8,07	8,03	7,88	7,86	7,82	7,79	7,82
	$\sigma_{\tau_{11,max}}$, мс	0,109	0,122	0,134	0,144	0,154	0,164	0,173	0,182	0,190	0,198
	$\frac{ \sigma_{\tau_{11}} - \sigma_{\tau_{11,max}} }{\sigma_{\tau_{11}}}$, %	4,28	4,21	4,13	4,12	4,10	4,02	4,01	3,99	3,97	3,99
0,02	T_s , мкс	166,67									
	τ_{strob} , пс	600									
	$N_{test.j}$	95	130	165	201	238	275	312	350	388	427
	$\overline{\tau_{11,max}}$, мс	2,54	3,46	4,41	5,38	6,37	7,37	8,37	9,38	10,41	11,42
	$\frac{ \overline{\tau_{11}} - \overline{\tau_{11,max}} }{\overline{\tau_{11}}}$, %	1,16	1,20	1,27	1,31	1,33	1,35	1,37	1,38	1,39	1,38
	$\sigma_{\tau_{11,max}}^2 \cdot 10^{-8}$	6,41	8,84	11,41	14,04	16,68	19,35	22,05	24,78	27,53	30,19
	$\frac{ \sigma_{\tau_{11}}^2 - \sigma_{\tau_{11,max}}^2 }{\sigma_{\tau_{11}}^2}$, %	5,90	5,75	5,48	5,32	5,25	5,18	5,11	5,08	5,04	5,09
	$\sigma_{\tau_{11,max}}$, мс	0,253	0,297	0,338	0,375	0,408	0,440	0,470	0,498	0,525	0,549
	$\frac{ \sigma_{\tau_{11}} - \sigma_{\tau_{11,max}} }{\sigma_{\tau_{11}}}$, %	2,99	2,92	2,78	2,70	2,66	2,63	2,59	2,57	2,55	2,58
0,05	T_s , мкс	500									
	τ_{strob} , пс	600									
	$N_{test.j}$	114	183	256	332	411	490	570	651	733	815
	$\overline{\tau_{11,max}}$, мс	10,71	17,21	24,14	31,33	38,70	46,16	53,75	61,40	69,15	76,88
	$\frac{ \overline{\tau_{11}} - \overline{\tau_{11,max}} }{\overline{\tau_{11}}}$, %	2,79	2,95	3,06	3,11	3,11	3,13	3,16	3,17	3,18	3,19
	$\sigma_{\tau_{11,max}}^2 \cdot 10^{-7}$	9,68	15,80	22,38	29,18	36,06	43,10	50,30	57,53	64,85	72,14
	$\frac{ \sigma_{\tau_{11}}^2 - \sigma_{\tau_{11,max}}^2 }{\sigma_{\tau_{11}}^2}$, %	0,26	0,74	1,10	1,26	1,23	1,30	1,40	1,44	1,47	1,49
	$\sigma_{\tau_{11,max}}$, мс	0,984	1,257	1,496	1,708	1,899	2,076	2,243	2,399	2,547	2,686
	$\frac{ \sigma_{\tau_{11}} - \sigma_{\tau_{11,max}} }{\sigma_{\tau_{11}}}$, %	0,13	0,37	0,55	0,63	0,61	0,65	0,70	0,72	0,73	0,74
0,10	T_s , мкс	1000									
	τ_{strob} , пс	600									
	$N_{test.j}$	140	256	383	517	655	796	939	1083	1229	1376
	$\overline{\tau_{11,max}}$, мс	30,31	55,49	83,15	112,18	142,20	172,72	203,69	235,14	266,81	298,79
	$\frac{ \overline{\tau_{11}} - \overline{\tau_{11,max}} }{\overline{\tau_{11}}}$, %	5,40	5,64	5,76	5,79	5,83	5,84	5,84	5,87	5,88	5,89
	$\sigma_{\tau_{11,max}}^2 \cdot 10^{-6}$	6,39	11,86	17,88	24,17	30,70	37,31	44,01	50,88	57,75	64,71
	$\frac{ \sigma_{\tau_{11}}^2 - \sigma_{\tau_{11,max}}^2 }{\sigma_{\tau_{11}}^2}$, %	9,01	9,66	10,01	10,09	10,21	10,22	10,23	10,32	10,33	10,37
	$\sigma_{\tau_{11,max}}$, мс	2,528	3,443	4,229	4,916	5,541	6,108	6,634	7,133	7,599	8,044
	$\frac{ \sigma_{\tau_{11}} - \sigma_{\tau_{11,max}} }{\sigma_{\tau_{11}}}$, %	4,41	4,72	4,89	4,93	4,98	4,98	4,99	5,03	5,04	5,05

Как и следовало ожидать, при неограниченном количестве тестов $N_{test.j} \rightarrow \infty$ среднее время тестирования больше $\overline{\tau_{11,max}} > \overline{\tau_{11}}$, по сравнению со средним

временем тестирования с ограничениями по количеству тестов. Так, отклонение среднего времени тестирования $\overline{\tau_{11}}$ от среднего времени тестирования при неограниченном количестве тестов $\overline{\tau_{11.max}}$ не превышает 0,72; 1,39; 3,19 и 5,89 % при обеспечении допустимых вероятностей ошибки синхронизации на уровне $P_{err.0}=0,01; 0,02; 0,05$ и 0,10 соответственно. Причём отклонение СКО $\widetilde{\sigma_{\tau_{11}}}$ от $\widetilde{\sigma_{\tau_{11.max}}}$ не выше 4,28; 2,99; 0,74 и 5,05 % при $P_{err.0}=0,01; 0,02; 0,05$ и 0,10 соответственно. Полученные аналитические выражения среднего $\overline{\tau_{11.max}}$ и СКО $\widetilde{\sigma_{\tau_{11.max}}}$ времени тестирования в сигнальном участке ВОЛС значительно проще полученных ранее аналитических выражений. В связи с незначительным отклонением результатов (менее 5,89 % для среднего времени тестирования и 5,05 % для СКО) полученные аналитические выражения могут быть использованы для расчёта среднего и дисперсии времени тестирования в сигнальном участке ВОЛС.

Сравнительный анализ полученных результатов с результатами моделирования (см. таблицу 3.11) этапа тестирования для 1-го участка ВОЛС показал незначительное отклонение. Так, отклонение расчётов относительно результатов моделирования составляет 2,7; 1,6; 0,2 и 3,1 % при $P_{err.0}=0,01; 0,02; 0,05$ и 0,10 соответственно. Таким образом, полученные аналитические выражения могут быть использованы для расчёта среднего и дисперсии времени тестирования в сигнальном участке ВОЛС.

Для оценки предельного (максимального) значения среднего времени тестирования введём нормирование

$$\overline{\tau_{11max.n}}(L_j) = \frac{\overline{\tau_{11.max}}(L_j)}{T_s} = \frac{1}{\overline{n_{s.j}}} = \frac{1}{\overline{n_{s.0}}} \cdot 10^{\frac{\alpha_{OF}[дБ/км] \cdot L_j[км]}{10}}.$$

Поскольку расстояние до станции неизвестно L_j , то принимается, что вероятность распределения срабатывания аппаратуры на дальности L_j равновероятна в пределах длины k -го сигнального участка ВОЛС

$$l_k = \begin{cases} L_1, & \text{при } k = 1; \\ L_k - L_{k-1}, & \text{при } k = \overline{2, N_{FOL}}. \end{cases}$$

Следовательно, для распределения вероятности справедлива формула $w(L_j) = 1/l_k = 1/(L_k - L_{k-1})$. Это позволяет рассчитать предельное среднее время тестирования в k-м сигнальном участке ВОЛС

$$\overline{\overline{\tau_{11.max.k.H}}} = \int_{L_{k-1}}^{L_k} w(L_j) \cdot \overline{\tau_{11.max.H}(L_j)} \cdot dL_j \rightarrow$$

$$\leftarrow = \frac{1}{l_k[\text{КМ}]} \cdot \frac{1}{\overline{n_{s.0}}} \cdot \frac{10}{\alpha_{OF} \left[\frac{\text{ДБ}}{\text{КМ}} \right] \cdot \ln(10)} \cdot \left[10^{\frac{\alpha_{OF}[\text{ДБ/КМ}] \cdot L_k[\text{КМ}]}{10}} - 10^{\frac{\alpha_{OF}[\text{ДБ/КМ}] \cdot L_{k-1}[\text{КМ}]}{10}} \right].$$

Результаты расчёта предельного значения среднего времени тестирования $\overline{\overline{\tau_{11.max.k.H}}}$ в сигнальном участке представлены в таблице 4.6.

Таблица 4.6 – Предельное значение среднего времени тестирования в k-м сигнальном участке ВОЛС

$P_{err.0}$	Параметр	Участок ВОЛС, k									
		1	2	3	4	5	6	7	8	9	10
0,01	T_s , мкс	83,33									
	τ_{strob} , пс	600									
	l_k , км	6,00	4,90	4,13	3,56	3,14	2,79	2,51	2,28	2,09	1,94
	$\overline{\tau_{11.max.H}}$, с	12,83	15,72	18,65	21,62	24,62	27,64	30,66	33,70	36,75	39,83
	$\overline{\overline{\tau_{11.max.k.H}}}$, с	11,35	14,22	17,14	20,10	23,08	26,10	29,12	32,16	35,20	38,27
0,02	T_s , мкс	166,67									
	τ_{strob} , пс	600									
	l_k , км	10,17	7,47	5,85	4,80	4,07	3,50	3,07	2,77	2,50	2,25
	$\overline{\tau_{11.max.H}}$, с	15,24	20,77	26,46	32,30	38,23	44,19	50,19	56,30	62,43	68,55
	$\overline{\overline{\tau_{11.max.k.H}}}$, с	12,44	17,86	23,50	29,28	35,18	41,14	47,13	53,18	59,31	65,44
0,05	T_s , мкс	500									
	τ_{strob} , пс	600									
	l_k , км	18,39	11,44	8,17	6,29	5,10	4,25	3,67	3,21	2,87	2,56
	$\overline{\tau_{11.max.H}}$, с	21,43	34,42	48,28	62,66	77,40	92,31	107,50	122,81	138,30	153,77
	$\overline{\overline{\tau_{11.max.k.H}}}$, с	14,99	27,41	40,96	55,16	69,77	84,64	99,71	114,98	130,40	145,89
0,10	T_s , мкс	1000									
	τ_{strob} , пс	600									
	l_k , км	26,75	14,59	9,76	7,23	5,72	4,69	3,98	3,46	3,05	2,73
	$\overline{\tau_{11.max.H}}$, с	30,31	55,49	83,15	112,18	142,20	172,72	203,69	235,14	266,81	298,79
	$\overline{\overline{\tau_{11.max.k.H}}}$, с	18,32	41,64	68,39	96,94	126,60	156,97	187,78	219,04	250,64	282,50

Величина $\overline{\overline{\tau_{11.max.k.H}}}$ усреднена по всем возможным позициям появления фотонного импульса в участке при неограниченном количестве тестов. Следовательно, $\overline{\overline{\tau_{11.max.k.H}}}$ всегда будет меньше $\overline{\tau_{11.max.H}}$, рассчитанной для верхних границ участков $\overline{\overline{\tau_{11.max.k.H}}} < \overline{\tau_{11.max.H}}$. Данное условие подтверждается данными таблицы 4.6. Так, отклонение $\overline{\tau_{11.max.H}}$ от $\overline{\overline{\tau_{11.max.k.H}}}$ не превышает 11,48; 18,39;

30,02 и 39,57 % при вероятности ошибки синхронизации $P_{err.0}=0,01; 0,02; 0,05$ и 0,10 соответственно. От участка к участку отклонение значительно сокращается и при $P_{err.0}=0,10$ в 1-м участке ВОЛС равно 39,57 %, во 2-м – 24,96 %, а в 10-м – всего 5,45 %. Значительное отклонение указанных величин в 1-м участке ВОЛС обусловлено наибольшей протяжённостью 1-го участка и, следовательно, наибольшим изменением среднего числа фотонов в импульсе $\overline{n_{s.j}}$.

Нормированное среднее время тестирования во всей ВОЛС может быть найдено по формуле

$$\overline{\tau_{test.H}} = \sum_{k=1}^{N_{FOL}} p_{reg.k} \cdot \overline{\tau_{11.max.k.H}},$$

где $p_{reg.k} = l_k/L_{FOL}$ – вероятность нахождения фотонного импульса в k -м участке.

Следовательно, среднее время тестирования во всей ВОЛС равно

$$\overline{\tau_{test}} = \overline{\tau_{test.H}} \cdot T_s.$$

Результаты расчёта вероятности нахождения фотонного импульса в k -м участке и среднего времени тестирования во всей ВОЛС при $\tau_{strob}=600$ пс представлены в таблице 4.7.

Нахождение фотонного импульса равновероятно по всей анализируемой длине ВОЛС. Вероятность попадания фотонного импульса в j -й участок равна отношению длины анализируемого участка к длине ВОЛС $p_{reg.j} = l_j/L_{FOL}$. В связи с уменьшением длины от участка к участку, вероятность $p_{reg.k}$ также уменьшается и достигает минимального значения в 10-м участке ВОЛС.

При ужесточении требований к вероятности ошибки синхронизации протяжённость ВОЛС значительно сокращается (см. таблицу 3.1). Следовательно, период следования синхроимпульсов также уменьшается. При уменьшении вероятности ошибки синхронизации в 10 раз (с 0,10 до 0,01) длина ВОЛС сокращается в 2,5 раза (82 км против 33,4 км), а период следования синхроимпульсов уменьшается в 12 раз (1000 мкс против 83,33 мкс). Поэтому при ужесточении требований к вероятности ошибки синхронизации среднее время тестирования во всей ВОЛС также значительно сокращается. Так, при $P_{err.0}=0,10$

среднее время тестирования во всей ВОЛС равно 85,01 мс, а при $P_{err.0}=0,01$ – всего 1,80 мс (в 47,2 раза меньше).

Таблица 4.7 – Среднее время тестирования во всей ВОЛС

$P_{err.0}$	Параметр	Участок ВОЛС, k									
		1	2	3	4	5	6	7	8	9	10
0,01	T_s , мкс	83,33									
	$p_{reg.k}$, %	18,01	14,70	12,39	10,67	9,41	8,37	7,51	6,84	6,27	5,82
	$\overline{\tau_{test.H}}$, с	21,58									
	$\overline{\tau_{test}}$, мс	1,80									
0,02	T_s , мкс	166,67									
	$p_{reg.k}$, %	21,89	16,08	12,59	10,34	8,76	7,53	6,61	5,96	5,38	4,85
	$\overline{\tau_{test.H}}$, с	30,42									
	$\overline{\tau_{test}}$, мс	5,07									
0,05	T_s , мкс	500									
	$p_{reg.k}$, %	27,88	17,34	12,38	9,54	7,73	6,45	5,57	4,87	4,35	3,88
	$\overline{\tau_{test.H}}$, с	52,61									
	$\overline{\tau_{test}}$, мс	26,30									
0,10	T_s , мкс	1000									
	$p_{reg.k}$, %	32,64	17,80	11,91	8,82	6,98	5,72	4,85	4,23	3,72	3,33
	$\overline{\tau_{test.H}}$, с	85,01									
	$\overline{\tau_{test}}$, мс	85,01									

Резюме. Проведён анализ статистических характеристик этапа тестирования в сигнальном участке ВОЛС. Определены количественно среднее и дисперсия времени тестирования с принятием решения об обнаружении при различных значениях допустимой вероятности ошибки синхронизации. При ужесточении требований к вероятности ошибки синхронизации в разы (с 0,10 до 0,01) среднее время тестирования значительно сокращается (в 47,2 раза) и составляет всего 1,8 мс. Получены аналитические выражения для экспресс-расчёта среднего и дисперсии времени тестирования в сигнальном участке ВОЛС, причём отклонение при экспресс-расчёте не превышает 5,89 % для среднего и 5,05 % для СКО времени тестирования.

4.6 Выводы к главе 4

Предложен графоаналитический метод расчёта среднего и дисперсии времени вхождения в синхронизм станций системы КРК для предлагаемого двухэтапного алгоритма синхронизации приёмопередающей и кодирующей

станций системы КРК. Получены диаграмма состояний и переходов, таблица, характеризующая вероятности переходов между состояниями системы.

Получены аналитические выражения для расчёта среднего времени вхождения в синхронизм станций предлагаемого алгоритма синхронизации графоаналитическим методом в общем случае при произвольном количестве участков, кадров и тестов, достоверность которых подтверждается незначительным отклонением от результатов моделирования (не более 2,8 %). Получены аналитические выражения для экспресс-расчёта среднего времени синхронизации графоаналитическим методом, причём отклонение при расчёте составляет не более 5,47 %. Отмечена вычислительная сложность применения графоаналитического метода для расчёта дисперсии времени синхронизации станций системы КРК.

Получены аналитические выражения для расчёта среднего и дисперсии времени тестирования алгоритма синхронизации станций системы КРК при произвольном количестве участков, кадров и тестов. Получены аналитические выражения для экспресс-расчёта среднего и дисперсии времени тестирования, причём отклонение результатов при экспресс-расчёте составляет не более 5,89 % для среднего времени тестирования и не более 5,05 % для СКО.

Результаты проведённых исследований отражены в статье [24].

ЗАКЛЮЧЕНИЕ

В результате проведённых диссертационных исследований достигнута поставленная цель – увеличение протяжённости ВОЛС в автокомпенсационной системе КРК на однофотонных лавинных фотодиодах (ЛФД) при сохранении энергетической скрытности синхронизации на основе протокола BB84 благодаря разбиению ВОЛС на участки с убывающей длиной.

Разработан новый двухэтапный алгоритм временной синхронизации приёмопередающей и кодирующей станций системы КРК, позволяющий при сохранении энергетической скрытности увеличить протяжённость ВОЛС в разы благодаря разбиению ВОЛС на участки с убывающей длиной, на верхних границах которых вероятность ошибки синхронизации не превышает заданного уровня. Так, например, при вероятности ошибки синхронизации 0,01; 0,02; 0,05 и 0,10 протяжённость ВОЛС увеличивается в 5,6; 4,5; 3,6 и 3,1 раза соответственно. Предложена структура аппаратуры, реализующей предлагаемый алгоритм.

Предложена методика расчёта временных и вероятностных характеристик предлагаемого алгоритма синхронизации, позволяющая оценить влияние частоты генерации ИТТ и вероятности ошибки синхронизации на протяжённость ВОЛС. Так, при ухудшении вероятности ошибки синхронизации в 10 раз (с 0,01 до 0,10) протяжённость ВОЛС увеличивается в 2,5 раза (82 против 33,4 км). При ухудшении характеристик ОЛФД (увеличении частоты генерации ИТТ) протяжённость ВОЛС значительно сокращается – увеличение частоты генерации ИТТ в ~10 раз (с 6 до 50 Гц) при гарантии вероятности ошибки синхронизации 0,10 приводит к сокращению длины ВОЛС в 2,2 раза (81,96 против 37,53 км).

Описана модель синхронизации согласно предложенному алгоритму в пакете прикладных программ MATLAB, позволяющая оценить влияние вероятности ошибки синхронизации на эффективность алгоритма. При ухудшении требований к вероятности ошибки синхронизации на порядок (с 0,01 до 0,10) среднее время вхождения в синхронизм увеличивается в десятки раз (в 28,9 раза – 62,57 против

2,16 мс). Ужесточение требований к вероятности ошибки синхронизации до 0,01 позволяет достичь синхронизации станций системы КРК в 1-м участке ВОЛС с вероятностью более 99%. Сравнительный анализ полученных результатов с теоретическими расчётами показал различие вероятности успешной синхронизации в 1-м участке ВОЛС не более 5% при различной допустимой вероятности ошибки синхронизации, что указывает на возможность использовать ранее полученные аналитические выражения.

Получены аналитические выражения для расчёта среднего времени синхронизации графоаналитическим методом при произвольном количестве участков, кадров и тестов. Отклонение результатов расчёта среднего времени синхронизации, полученных с помощью графоаналитического метода, от результатов моделирования не превышает 2,8 %. Незначительное отклонение указывает на возможность использовать полученные аналитические выражения для расчёта среднего времени синхронизации станций системы КРК согласно предложенному алгоритму. Получены аналитические выражения для экспресс-расчёта среднего времени синхронизации графоаналитическим методом. Экспресс-расчёт значительно проще полученных ранее выражений. Учитывая незначительное отклонение результатов (не более 5,47 % при экспресс-расчёте), полученные выражения могут применяться для экспресс-расчёта среднего времени синхронизации.

Разработаны два программных продукта для ЭВМ, защищённые авторскими свидетельствами, позволяющие анализировать характеристики предложенного двухэтапного алгоритма синхронизации. Во-первых, оценить характеристики каждого из участков ВОЛС с убывающей длиной, а также вероятностные и энергетические характеристики алгоритма синхронизации. Во-вторых, провести моделирование этапа тестирования подсистемы синхронизации с оценкой временных и вероятностных характеристик.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Gisin, N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // *Reviews of Modern Physics*. – 2002. – Vol. 74. – № 1. – P. 145-195.
2. Bennett, C. Quantum cryptography: Public key distribution and coin tossing / C. Bennett, G. Brassard // *Proceedings of IEEE international conference on computers, systems and signal processing*. – 1984. – P. 175-179.
3. Shor, P. W. Simple proof of security of the BB84 quantum key distribution protocol / P. W. Shor, J. Preskill // *Physical Review Letters*. – 2000. – Vol. 85. – P. 441-444.
4. Gerhardt, I. Full-field implementation of a perfect eavesdropper on a quantum cryptography system / I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov // *Nat. Commun.* – 2011. – P. 349.
5. Lydersen, L. Hacking commercial quantum cryptography systems by tailored bright illumination / L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov // *Nature Photonics*. – 2010. – № 4. – P. 686-689.
6. Makarov, V. Controlling passively quenched single photon detectors by bright light / V. Makarov // *New Journal of Physics*. – 2009. – Vol. 11. – P. 065003.
7. Gisin, N. Trojan-horse attacks on quantum-key-distribution systems / N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy // *Physical Review A*. – 2006. – Vol. 73. – P. 022320.
8. Румянцев, К. Е. Синхронизация в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений / К. Е. Румянцев // *Телекоммуникации*. – 2017. – № 2. – С. 32-40.
9. Румянцев, К. Е. Защита процесса синхронизации в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений / К. Е. Румянцев // *Телекоммуникации*. – 2017. – № 3. – С. 36-44.
10. Гальярди, Р. М., Ш., Карп. Оптическая связь. – М.: Связь. – 1978. – 424 с.

11. Витерби, Э. Д. Принципы когерентной связи. – М.: Сов. радио. – 1970. – 392 с.
12. Стиффлер, Дж. Теория синхронной связи. – М.: Связь. – 1975. – 488 с.
13. Lindsey, W. C. Synchronization Systems in Communication and Control: монография. – Prentice-Hall, Englewood Cliffs, New Jersey. – 1972. – 695 p.
14. Румянцев, К. Е. Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости / К. Е. Румянцев, А. П. Плёткин // Известия ЮФУ. Технические науки. – 2014. – № 8. – С. 81-96.
15. Румянцев, К. Е. Синхронизация системы квантового распределения ключа в режиме однофотонной регистрации импульсов для повышения защищённости / К. Е. Румянцев, А. П. Плёткин // Радиотехника. – 2015. – № 2. – С. 125-134.
16. Миронов, Я. К. Формулирование требований к протяжённости волоконно-оптической линии при внедрении двухэтапного алгоритма синхронизации в системе квантового распределения ключа / Я. К. Миронов, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2019. – №5 (207). – С. 6-16.
17. Миронов, Я. К. Вероятностные характеристики порогового алгоритма обнаружения синхроимпульсов в системе квантового распределения ключа на основе информации со смежной пары временных сегментов / Я. К. Миронов, П. Д. Миронова, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2020. – №4 (214). – С. 221-229.
18. Линенко, П. Д. Разбиение временного кадра на интервалы в системе квантового распределения ключа / П. Д. Линенко, Я. К. Миронов, К. Е. Румянцев // V Всероссийская научно-техническая конференция молодых ученых, аспирантов, магистрантов и студентов "Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности" :сборник статей Всероссийской научно-технической конференции, 01-07 апреля 2019 г. – Таганрог, 2019. – С. 82-84.

19. Миронов, Я. К. Исследование характеристик алгоритма синхронизации системы квантового распределения ключа на основе сравнения числа отсчетов со смежной пары временных окон с пороговым уровнем / Я. К. Миронов, П. Д. Миронова, К. Е. Румянцев // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации : сборник докладов II Всероссийской научной конференции (с приглашением зарубежных ученых), Ставрополь, Россия Ноябрь 30, 2020. – Ставрополь : СКФУ, 2020. – С. 219-226.

20. Миронов, Я. К. Алгоритм синхронизации станций автокомпенсационной волоконно-оптической системы квантового распределения ключа с разбиением волоконно-оптической линии на участки с убывающей длиной / Я. К. Миронов // Digital Era : материалы I Всероссийской научно практической конференции. – Грозный: Чеченский государственный университет, 2021. – С. 94-98. – DOI: 10.36684/38-2021-1-94-98.

21. Миронов, Я. К. Вероятностные характеристики порогового алгоритма обнаружения синхроимпульсов в системе квантового распределения ключа на основе информации со смежной пары временных сегментов / Я. К. Миронов, П. Д. Миронова, К. Е. Румянцев // Компьютерные и информационные технологии в науке, инженерии и управлении : материалы Всероссийской научно-технической конференции с международным участием имени профессора О. Н. Пьявченко "КомТех-2020" : в двух томах. Т. 1. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. – С. 54-61.

22. Rumyantsev, K. Y. Single Photon Algorithm of Search of a Pulse Radiation Source / K. Y. Rumyantsev, K. B. Bamatgireeva, Y. K. Mironov // Communications in Computer and Information Science. – 2019. – Т. 958. – P. 95-108. – DOI: 10.1007/978-981-13-3804-5_8.

23. Mironov, Y. K. Single-Photon Algorithm for Synchronizing the System of Quantum Key Distribution with Polling Sections of a Fiber-Optic Line / Y. K. Mironov, K. E. Rumyantsev // Communications in Computer and Information Science. – 2020. – Т. 1206. – P. 87-97. – DOI: https://doi.org/10.1007/978-981-15-4451-4_8.

24. Mironov, Y. K. Methodology for calculating the average time of entry into synchronism of stations of the system of quantum key distribution with sequential polling of fiber-optic line sections with decreasing length by the graphic-analytical method / Y. K. Mironov, P. D. Mironova, K. E. Rumyantsev // E3S Web of Conferences. – 2020. – Vol. 224. – P. 01032 (p. 1-9). – DOI: 10.1051/e3sconf/202022401032.

25. Mironov, Y. Characteristics of a two-stage synchronization algorithm in the system of quantum key distribution with dividing a fiber-optic line into sections with decreasing length / Y. Mironov, P. Mironova, K. Rumyantsev // ACM International Conference Proceeding Series. – 2020. – P. 3433596 (p. 1-5). – DOI: 10.1145/3433174.3433595.

26. Mironov, Y. K. Providing the Required Probability of Synchronization Error When Splitting a Fiber-Optic Line into Sections with Decreasing Length in a Quantum Key Distribution System / Y. K. Mironov, K. E. Rumyantsev // Proceedings - 2021 3rd International Conference on System Reliability and Safety Engineering, SRSE 2021. – 2021. – P. 145-149. – DOI: 10.1109/SRSE54209.2021.00032.

27. Свидетельство о государственной регистрации программы для ЭВМ № 2021618865 Российская Федерация. Программа разбиения волоконно-оптической линии подсистемы синхронизации системы квантового распределения ключа на участки с убывающей длиной : № 2021617523 : заявл. 20.05.2021 : опубл. 01.06.2021 / Я. К. Миронов, К. Е. Румянцев ; правообладатель федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет».

28. Свидетельство о государственной регистрации программы для ЭВМ № 2022615010 Российская Федерация. Программа моделирования этапа тестирования подсистемы синхронизации системы квантового распределения ключа при разбиении волоконно-оптической линии на участки с убывающей длиной : № 2022614701 : заявл. 25.03.2022 : опубл. 29.03.2022 / Я. К. Миронов, К. Е. Румянцев ; правообладатель федеральное государственное автономное образовательное учреждение высшего образования "Южный федеральный университет".

29. Shannon, C. E. A mathematical theory of communication / C. E. Shannon // ACM SIGMOBILE Mob. Comput. – 2001. – № 27. – P. 379-423.
30. Румянцев, К. Е. Квантовые технологии в телекоммуникационных системах: учебник. – Ростов-на-Дону: Южный федеральный университет, 2021. – 346 с.
31. Hughes, R. J. Quantum cryptography / R. J. Hughes et al. // Contemp. Phys. – 1995. – № 36 (3). – P. 149-163.
32. Румянцев, К. Е. Системы квантового распределения ключа: учебное пособие. – Ростов-на-Дону: Южный федеральный университет, 2011. – 264 с.
33. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring / P. W. Shor // Proc. 35th Annu. Symp. Found. Comput. Sci. – 1994. – P. 124-134.
34. Кронберг, Д. А., Ожигов, Ю. И., Чернявский, А. Ю. Квантовая криптография: учебное пособие. – М.: МГУ имени М. В. Ломоносова. – 112 с.
35. Tanga, X. Performance of continuous variable quantum key distribution system at different detector bandwidth / X. Tanga, R. Kumarb, S. Rena, A. Wonfora, R.V. Pentya, I.H. Whiteac // Optics Communications. – 2020. – № 471. – P. 126034.
36. Rameez, A. Seamless Cryptographic Key Generation via Off-the-Shelf Telecommunication Components for End-to-End Data Encryption / Rameez Asif, William J. Buchanan // Conference: IEEE International Conference on Internet of Things (iThings-2017). – 2017. – P. 910-916.
37. Stucki, D. Continuous high speed coherent one-way quantum key distribution / D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, H. Zbinden // Opt. Express. – 2009. – № 17 (16). – P. 13326-13334.
38. Qi, B. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers / B. Qi, L.-L. Huang, L. Qian, H.-K. Lo // Phys. Rev. A. – 2007. – № 76. – P. 052323.
39. Leverrier, A. Multidimensional reconciliation for a continuous-variable quantum key distribution / A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, P. Grangier // Phys. Rev. A. – 2008. – № 77. – P. 042325.

40. Chi, Y.-M. A balanced homodyne detector for highrate gaussian-modulated coherent-state quantum key distribution / Y.-M. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, S.-H. Youn, A. I. Lvovsky, L. Tian // *New Journal of Physics*. – 2011. – № 13 (1). – P. 013003.
41. Comandar, L. C. Room temperature single-photon detectors for high bit rate quantum key distribution / L. C. Comandar, B. Frauhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Pentty, A. J. Shields // *Applied Physics Letters*. – 2014. – № 104 (2). – P. 1-14.
42. Frohlich, B. Long-distance quantum key distribution secure against coherent attacks / B. Frohlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, A. J. Shields // *Optica*. – 2017. – № 4 (1). – P. 163-167.
43. Bennett, C. Quantum cryptography using any two non-orthogonal states / C. Bennett // *Physical Review Letters*. – 1992. – № 68. – P. 3121-3124.
44. Huttner, B. Quantum cryptography with coherent states / B. Huttner, N. Imoto, N. Gisin, T. Mor // *Physical Review A*. – 1995. – № 51. – P. 1863-1869.
45. Bruss, D. Optimal eavesdropping in quantum cryptography with six states / D. Bruss // *Physical Review Letters*. – 1998. – № 81. – P. 3018.
46. Goldenberg, L. Quantum cryptography based on orthogonal states / L. Goldenberg, L. Vaidman // *Physical Review Letters*. – 1995. – № 75. – P. 1239-1243.
47. Koashi, M. Quantum cryptography based on split transmission of one-bit information in two steps / M. Koashi, N. Imoto // *Physical Review Letters*. – 1997. – № 79. – P. 2383.
48. Scarani, V. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementation / V. Scarani, A. Acin, G. Ribordy, N. Gisin // *Phys. Rev. Lett.* – 2002. – № 92. – P. 057901.
49. Stucki, D. Quantum Key Distribution over 67 km with a plug & play system / D. Stucki et al. // *Quantum Phys.* – 2002. – № 8.
50. Muller, A. Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km / A. Muller, J. Breguet, N. Gisin // *Europhys. Lett.* – 2007. – № 23 (6). – P. 383-388.

51. Muller, A. “Plug and play” systems for quantum cryptography / A. Muller et al. // Appl. Phys. Lett. – 1997. – № 70. – P. 793-795.

52. Рупасов, А. В. Согласованная система квантовой рассылки криптографического ключа на поднесущей частоте модулированного света / А. В. Рупасов, А. В. Глейм, В. И. Егоров, Ю. Т. Мазуренко // Научно-технический Вестник СПбГУ ИТМО. – 2011. – Т. 2, № 72. – С. 95-99.

53. Stucki, D. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres / D. Stucki et al. // New J. Phys. – 2009. – № 11. – P. 1-9.

54. Lodewyck, J. Quantum key distribution over 25 km with an all-fiber continuous-variable system / J. Lodewyck et al. // Phys. Rev. A - At. Mol. Opt. Phys. – 2007. – № 76. – P. 1-10.

55. Korzh, B. Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre / B. Korzh et al. // Nat. Photonics. – 2014. – № 9 (3). – P. 7.

56. idQuantique. Clavis2 datasheet IDQuantique v 1.2 / idQuantique. – 2008. – 47 p.

57. Tokyo QKD Network: [сайт]. – URL: <http://www.nict.go.jp/en/press/2010/10/14-1.html#w1> (дата обращения: 01.12.2020). – Текст: электронный.

58. Зензин, О. С. Стандарт криптографической защиты AES. Конечные поля / О. С. Зензин, М. А. Иванов. – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.

59. Rumyantsev, K. E. Modeling of Quantum Key Distribution System for Secure Information Transfer / K. E. Rumyantsev, D. M. Golubchikov // Integrated Models for Information Communication Systems and Networks: Design and Development. – 2013. – P. 314-342.

60. Clavis300 QKD Brochure: [сайт]. – URL: https://marketing.idquantique.com/acton/attachment/11868/f-42e4a1b3-46a2-4f2f-8fcd-ba9118954c3a/1/-/-/-/Clavis300_QKD_Brochure.pdf (дата обращения: 08.12.2020). – Текст: электронный.

61. Cerberis QKD System Brochure: [сайт]. – URL: <https://marketing.idquantique.com/acton/attachment/11868/f-021a/1/-/-/-/>

/Cerberis%20QKD%20System_Brochure.pdf (дата обращения: 08.12.2020). – Текст: электронный.

62. Clavis3 QKD Platform Brochure: [сайт]. – URL: https://marketing.idquantique.com/acton/attachment/11868/f-0216/1/-/-/-/-/Clavis3%20QKD%20Platform_Brochure.pdf (дата обращения: 08.12.2020). – Текст: электронный.

63. Cerberis XG QKD System Flyer: [сайт]. – URL: https://marketing.idquantique.com/acton/attachment/11868/f-a0520638-89bf-4abb-89f6-d6c1ff482d22/1/-/-/-/-/Cerberis%20XG%20QKD%20System_Flyer.pdf (дата обращения: 10.12.2020). – Текст: электронный.

64. Cerberis XGR Brochure: [сайт]. – URL: https://marketing.idquantique.com/acton/attachment/11868/f-5f50c28e-bac2-40a7-bc5a-30971c980753/1/-/-/-/-/Cerberis%20XGR_Brochure.pdf (дата обращения: 10.12.2020). – Текст: электронный.

65. IDQ unveils Cerberis XGR QKD Platform: [сайт]. – URL: <https://www.idquantique.com/idq-unveils-cerberis-xgr/> (дата обращения: 10.12.2020). – Текст: электронный.

66. Centauris CN9000 Series Brochure: [сайт]. – URL: https://marketing.idquantique.com/acton/attachment/11868/f-021c/1/-/-/-/-/Centauris%20CN9000%20Series_Brochure.pdf (дата обращения: 10.12.2020). – Текст: электронный.

67. Centauris CN6000 Series Brochure: [сайт]. – URL: https://marketing.idquantique.com/acton/attachment/11868/f-0217/1/-/-/-/-/Centauris%20CN6000%20Series_Brochure.pdf (дата обращения: 10.12.2020). – Текст: электронный.

68. 2016 04 IDQ Datasheet Centauris: [сайт]. – URL: https://marketing.idquantique.com/acton/attachment/11868/f-0219/1/-/-/-/-/Centauris%20Series_Brochure.pdf (дата обращения: 10.12.2020). – Текст: электронный.

69. Centauris CV1000 Brochure: [сайт]. – URL: https://marketing.idquantique.com/acton/attachment/11868/f-0318/1/-/-/-/-/Centauris%20CV1000_Brochure.pdf (дата обращения: 10.12.2020). – Текст: электронный.

70. QPN 5505. User's manual. MagiQ Technologies, Inc / MagiQ Technologies, Inc. – 2004. – 62 p.

71. Hammond, A. MagiQ and Verizon Smash Distance and Cost Barriers with world's longest cascaded network for practical quantum cryptography / A. Hammond // New Technology Enables Ultra Secure Communications. MagiQ Technologies, Inc. – 2006.

72. Zavriyev, A. Quantum Cryptography Realized or Are we entangled yet? / A. Zavriyev // MagiQ Technologies, Inc. – 2009.

73. Слепов, Н. Н. Квантовая криптография: передача квантового ключа. Проблемы и решения / Н. Н. Слепов // Электроника: наука, технология, бизнес. – 2006. – Т. 2. – С. 54-61.

74. Квантовая криптография: идеи и практика: монография / Под ред. С. Я. Килина, Д. Б. Хорошко, А. П. Низовцева. – Минск: Беларуская навука, 2008. – 392 с.

75. Bennet, C. H. Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States / C. H. Bennet, S. J. Wiesner // Physical Review Letters. – 1992. – № 69. – P. 2881.

76. Bennett, Ch. H. Experimental quantum cryptography / Ch. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin // Journal of Cryptology. – 1992. – № 5. – P. 3-28.

77. Курочкин, В. Л. Экспериментальная установка для квантовой криптографии с одиночными поляризационными фотонами / В. Л. Курочкин, И. И. Рябцев, И. Г. Неизвестный // Журнал технической физики. – 2005. – Т. 75, № 6. – С. 54-58.

78. Плёткин, А. П. Исследование режима вхождения в синхронизм при использовании фотонных импульсов системы квантового распределения ключа /

А. П. Плёткин // Физико-математические методы и информационные технологии в естествознании, технике и гуманитарных науках: сборник материалов международного научного е-симпозиума. – 2015. – С. 101-113.

79. Румянцев, К. Е. Исследование подсистемы синхронизации системы квантового распределения ключа QPN 5505 / К. Е. Румянцев, Е. А. Рудинский // Информатизация и связь. – 2018. – № 4. – С. 12-17.

80. Howell M., Vig H. Sentinel synchronization method for enhancing QKD security (Способ синхронизации для повышения безопасности квантового распределения ключа) // Патент US7436961 / патентообладатель Magiq Technologies, Inc.; заявл. 8.03.2005; опубл. 14.10.2008.

81. System and method for providing two-way communication of quantum signals, timing signals, and public data (Система и способ обеспечения двустороннего обмена квантовыми сигналами, сигналами синхронизации и данными общего пользования) // Патент US7437081 / патентообладатель Magiq Technologies, Inc.; заявл. 1.11.2004; опубл. 14.10.2008.

82. Rumyantsev, K. E. Single-photon Synchronization Mode of Quantum Key Distribution System / К. Е. Rumyantsev, A. P. Pljonkin // 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). – 2016. – P. 1-6.

83. Курочкин, В. Л. Экспериментальные исследования в области квантовой криптографии / В. Л. Курочкин // Фотоника. – 2012. – Т. 5. – С. 54-66.

84. Salvail, L. Security of trusted repeater quantum key distribution networks / L. Salvail et al. // Journal of Computer Security. – 2010. – № 18 (1). – P. 61-87.

85. Cabello, A. Quantum key distribution without alternative measurements / A. Cabello // Physical Review A. – 2000. – № 61 (5). – P. 1-4.

86. Hiskett, P. A. Long-distance quantum key distribution in optical fibre / P. A. Hiskett et al. // New Journal of Physics. – 2006. – № 8. – P. 1-7.

87. Patel, K.A. Coexistence of high-bit-rate quantum key distribution and data on optical fiber / K. A. Patel et al. // Physical Review X. – 2012. – № 2 (4). – P. 1-8.

88. Gobby, G. Unconditionally secure quantum key distribution over 50 km of standard telecom fibre / G. Gobby, Z. L. Yuan, A. J. Shields // Electronics Letters. – 2004. – № 40. – P. 1603-1605.

89. Gottesman, D. Security of quantum key distribution with imperfect devices / D. Gottesman, H. K. Lo, N. Lutkenhaus, J. Preskill // Proceedings of International Symposium On Information Theory. – 2004. – № 136.

90. Rudinsky, E. Graph-analytical method for estimating single-photon synchronization parameters of an auto-compensation quantum key distribution system / E. Rudinsky, K. Rumyantsev // 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC'18). – 2018. – P. 765-769.

91. Plenkin, A. Comparative analysis of single-photon synchronization algorithms in the quantum key distribution system / A. Plenkin, K. Rumyantsev, E. Rudinsky // 2017 IEEE East-West Design & Test Symposium (EWDTS'17). – 2017.

92. Rumyantsev, K. E. Evaluation of the Influence of the Dispersion Properties of a Fiber-Optic Line on the Efficiency of an Algorithm for Single-Photon Synchronization of Quantum Key Distribution System / K. E. Rumyantsev, P. D. Linenko, H. H. -Sh. Shakir // Conference Proceedings - Radiation and Scattering of Electromagnetic Waves, RSEMW 2019. – 2019. – P. 392-395.

93. Pljonkin, A. Preliminary Stage Synchronization Algorithm of Auto-compensation Quantum Key Distribution System with an Unauthorized Access Security / A. Pljonkin, K. Rumyantsev // Proceeding of the 15th International Conference on Electronics, Information, and Communication 2016 (ICEIC 2016). – 2016. – Paper № 1570220423.

94. Румянцев, К. Е. Эффективность синхронизации системы квантового распределения ключа на однофотонных лавинных фотодиодах / К. Е. Румянцев, А. П. Плёнкин // Известия ЮФУ. Технические науки. – 2016. – № 9 (182). – С. 4-15.

95. Румянцев, К. Е. Безопасность режима синхронизации системы квантового распределения ключей / К. Е. Румянцев, А. П. Плёнкин // Известия ЮФУ. Технические науки. – 2015. – № 5 (166). – С. 135-153.

96. Rumyantsev, K. E. Synchronization Safety Problem in Quantum Key Distribution System / K. E. Rumyantsev, A. P. Pljonkin // Proceedings of the International Conference on Electronics, Information, and Communication (ICEIC'17). – 2017.

97. Румянцев, К. Е. Двухэтапный временной алгоритм синхронизации в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений / К. Е. Румянцев, Е. А. Рудинский // Известия ЮФУ. Технические науки. – 2017. – №5 (190). – С. 75-89.

98. Rudinsky, E. Time synchronization method in quantum key distribution system with automatic compensation of polarization distortions / E. Rudinsky, K. Rumyansev // 2017 2nd International Conference on Multimedia and Image Processing (ICMIP'17). – 2017. – С. 346-349.

99. Rumyansev, K. Parameters of the two-stage synchronization algorithm for the quantum key distribution system / K. Rumyansev, E. Rudinsky // Proceedings of the 10th International Conference on Security of Information and Networks (SIN'17). – 2017. – С. 140-147.

100. Quantum cryptography key distributing system and synchronizing method used in the same (Криптографическая система КРК и способ синхронизации, используемый в ней) // Патент US-7869599-B2 / патентообладатель Nec Corporation; заявл. 11.10.2004; опубл. 10.01.2011.

101. Communication system and synchronization control method (Система коммуникации и способ управления синхронизации) // Патент US 20070058810 A1 / Akihiro T., Akio T., Seigo T., Wakakon M.; опубл. 15.03.2007.

102. Temperature independent QKD system using alternative-shifted phase modulation method // Патент 2004-335228 / Tanaka A.; зарегистр. 19.11.2006.

103. Tomita, A. Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm / A. Tomita // Optics letters. – 2002. – Vol. 27. – P. 1827-1829.

104. Рудинский, Е. А. Экспериментальное исследование систем квантового распределения ключей в режиме установления связи при изменении условий

распространения и обработки фотонов: выпускная квалификационная работа / Е. А. Рудинский. – Таганрог: ИТА ЮФУ, 2018.

105. Миронов, Я. К. Синхронизация станций системы квантового распределения ключа с последовательным опросом участков волоконно-оптической линии с убывающей длиной / Я. К. Миронов // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности : VII Всероссийская научно-техническая конференция : сборник статей Всероссийской научно-технической конференции, 5-11 апреля 2021. – Таганрог, 2021. – С. 109-112.

106. Румянцев, К. Е., Shakir, Н. Н. Проектирование системы квантового распределения ключа с интерферометрами Маха-Цендера: учебное пособие. – Таганрог: Издательство Южного федерального университета, 2020. – 108 с.

107. ID210 advanced system for single photon detection with 100MHz gated mode and free-running mode: [сайт]. – URL: <https://www.photonicsolutions.co.uk/upfiles/id210-specs.pdf> (дата обращения: 12.02.2021). – Текст: электронный.

108. ID230 free-running InGaAs/InP photon counter with 50Hz dark count rate at 10% quantum efficiency: [сайт]. – URL: <https://www.photonicsolutions.co.uk/upfiles/id230-specs.pdf> (дата обращения: 12.02.2021). – Текст: электронный.

109. ID280 superconducting nanowire with 70% quantum efficiency and fastest electronics: [сайт]. – URL: <https://oessp.ru/upload/oessp/images/pdf/files/idquantique/id280-datasheet.pdf> (дата обращения: 12.02.2021). – Текст: электронный.

110. Прудников, А. П., Брычков, Ю. А., Маричев, О. И. Интегралы и ряды элементарные функции: монография. – М.: Главная редакция физико-математической литературы, 1981. – 800 с.

111. Greenberg, J. S. On the Narrow Beam Communication System Acquisition Problem / J. S. Greenberg // IEEE Trans. – 1964. – Vol. MIL-8. – P. 28.

112. Шереметьев, А. Г. Оценка эффективности оптимальных адаптивных приемников оптического диапазона / А. Г. Шереметьев, Е. М. Калугин // 4-я Всесоюзная конференция по теории передачи и кодирования информации, секция II, г. Ташкент. – 1969.

113. Шереметьев, А. Г. Статистическая теория лазерной связи: монография. – М.: Связь, 1971. – 264 с.

ПРИЛОЖЕНИЕ А. ЛИСТИНГ ПРОГРАММ МАТЛАВ ДЛЯ ПРОЕКТИРОВАНИЯ МОДУЛЯ ДВУХЭТАПНОЙ ОДНОФОТОННОЙ СИНХРОНИЗАЦИИ

Программа разбиения волоконно-оптической линии подсистемы синхронизации системы квантового распределения ключа на участки с убывающей длиной

Программа предназначена для оценки методом имитационного моделирования характеристик алгоритма синхронизации станций системы квантового распределения ключа. Отличительной особенностью предлагаемого алгоритма является разбиение для анализа волоконно-оптической линии связи на участки с убывающей длиной. Благодаря этому уровень импульсов темнового тока значительно уменьшается от участка к участку. При этом отношение сигнал-шум на всех верхних границах участков равны задаваемому значению. Следовательно, увеличивается отношение сигнал/шум и, как следствие, расстояние передачи, на котором гарантируется вхождение в синхронизм приёмопередающей и кодирующей станций. Поиск фотонного импульса осуществляется в два этапа: этап поиска и этап тестирования. На этапе поиска участки последовательно анализируются, причём каждому участку соответствует определенное число кадров. При регистрации фотонного импульса аппаратура переходит к этапу тестирования, в котором в течение заданного числа тестов производится повторный опрос участка. При повторной регистрации фотонного импульса процесс синхронизации считается успешно завершённым. Основная область применения программы – моделирование процесса синхронизации станций системы квантового распределения ключа посредством обнаружения синхроимпульса. Функциональные возможности программы: задаются исходные параметры передающего и приемного устройств, линии связи; на выходе рассчитываются вероятностные и энергетические характеристики предлагаемого алгоритма синхронизации.

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2021618865

**Программа разбиения волоконно-оптической линии
подсистемы синхронизации системы квантового
распределения ключа на участки с убывающей длиной**

Правообладатель: *федеральное государственное автономное
образовательное учреждение высшего образования
«Южный федеральный университет» (RU)*

Авторы: *Миронов Яков Константинович (RU), Румянцев
Константин Евгеньевич (RU)*

Заявка № 2021617523

Дата поступления 20 мая 2021 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 01 июня 2021 г.



Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

***Программа моделирования этапа тестирования подсистемы
синхронизации системы квантового распределения ключа при разбиении
волоконно-оптической линии на участки с убывающей длиной***

Программа предназначена для оценки методом имитационного моделирования характеристик этапа тестирования алгоритма синхронизации станций системы квантового распределения ключа при разбиении волоконно-оптической линии на участки с убывающей длиной. Алгоритм синхронизации станций системы квантового распределения ключа включает поиск фотонного импульса, который осуществляется в два этапа: этап поиска и этап тестирования. Этап поиска состоит в последовательном анализе участков волоконно-оптической линии на предмет регистрации фотонного импульса. При регистрации фотонного импульса аппаратура переходит к этапу тестирования, в течение которого производится повторный опрос предположительно сигнального участка. В случае повторной регистрации фотонного импульса на этапе тестирования процесс грубой оценки момента приема фотонного импульса считается завершенным. Основная область применения программы – моделирование этапа тестирования алгоритма синхронизации станций системы квантового распределения ключа. Функциональные возможности программы: задаются исходные параметры передающего и приемного устройств, линии связи; на выходе рассчитываются вероятностные и временные характеристики этапа тестирования предлагаемого алгоритма синхронизации.

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022615010

Программа моделирования этапа тестирования подсистемы синхронизации системы квантового распределения ключа при разбиении волоконно-оптической линии на участки с убывающей длиной

Правообладатель: *федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (RU)*

Авторы: *Миронов Яков Константинович (RU), Румянцев Константин Евгеньевич (RU)*



Заявка № 2022614701

Дата поступления 25 марта 2022 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 29 марта 2022 г.

*Руководитель Федеральной службы
по интеллектуальной собственности*

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 68b80077e14e40f0a94edbd24145d5c7
Владелец **Зубов Юрий Сергеевич**
Действителен с 26.05.2022 по 26.05.2023

Ю.С. Зубов

ПРИЛОЖЕНИЕ Б. СЕРТИФИКАТЫ





Confirmation of Participation

Yakov Mironov
Southern federal university

has participated in the
**13th International Conference on Security of
Information and Networks**

SIN 2020

**Istanbul, Turkey
November 04-07, 2020**

Prof. Dr. Berna Örs Yalçın
Chair, SIN 2020
Istanbul Technical University

SIN 2020

<https://www.sinconf.org/>



МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ



ДИПЛОМ

вручается

Миронову Я. К.

за лучший доклад
в I Всероссийской научно-практической
конференции «Digital Era»

Проректор
по науке и инновациям
ФГБОУ ВО «Чеченский
государственный университет»
М.Р. Нахаев



26 марта 2021 г. - Грозный

СЕРТИФИКАТ

участника конференции

VII Всероссийской научно-технической конференции
«Фундаментальные и прикладные аспекты компьютерных
технологий и информационной безопасности»

МИРОНОВ ЯКОВ КОНСТАНТИНОВИЧ

Руководитель: Румянцев Константин Евгеньевич

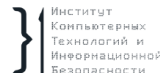
Секция: Информационная безопасность
телекоммуникационных систем

Директор ИКТИБ



Г.Е. Веселов

рег. № 705.15.01–52/371



ИРТСУ
ИНСТИТУТ РАДИОТЕХНИЧЕСКИХ
СИСТЕМ И УПРАВЛЕНИЯ

Сертификат участника

КомТех-2020

Всероссийская научно-техническая конференция с международным участием
имени профессора О.Н. Пьявченко
“Компьютерные и информационные технологии в науке, инженерии и управлении”

Сертификат выдан

Миронову Якову Константиновичу

за представление доклада на секционном заседании конференции КомТех-2020
г. Таганрог, июнь 2020 года

Председатель Оргкомитета
конференции
Директор Института
радиотехнических систем и
управления



А.С. Болдырев

ПРИЛОЖЕНИЕ В. АКТЫ ВНЕДРЕНИЯ



УТВЕРЖДАЮ

Директор Института
компьютерных технологий
и информационной безопасности

Г.Е.Веселов

« 28 » апреля 2022 г.

Акт внедрения результатов диссертационной работы

Результаты диссертационных исследований аспиранта кафедры ИБТКС Миронова Якова Константиновича, посвященные разработке алгоритма энергетической скрытности синхронизации станций автокомпенсационной волоконно-оптической системы квантового распределения ключа на однофотонном лавинном фотодиоде, использованы при выполнении вузом гранта РФФИ № 20-37-90040, использованы при создании программ для ЭВМ, защищенных регистрацией Федеральной службой по интеллектуальной собственности:

Миронов Яков Константинович, Румянцев Константин Евгеньевич. Программа разбиения волоконно-оптической линии подсистемы синхронизации системы квантового распределения ключа на участки с убывающей длиной. Свидетельство о государственной регистрации программы для ЭВМ. Номер свидетельства: RU 2021618865. Патентное ведомство: Россия. Год публикации: 2021. Номер заявки: 2021617523. Дата регистрации: 20.05.2021. Дата публикации: 01.06.2021. Язык программирования: MATLAB. Объем: 20 КБ. Правообладатели: федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет».

Программа предназначена для оценки методом имитационного моделирования характеристик алгоритма синхронизации станций системы квантового распределения ключа. Отличительной особенностью предлагаемого алгоритма является разбиение для анализа волоконно-оптической линии связи на участки с убывающей длиной. Благодаря этому уровень импульсов темнового тока значительно уменьшается от участка к участку. При этом отношение сигнал-шум на всех верхних границах участков равны задаваемому значению. Следовательно, увеличивается отношение сигнал/шум и, как следствие, расстояние передачи, на котором гарантируется вхождение в синхронизм приёмопередающей и кодирующей станций.

Поиск фотонного импульса осуществляется в два этапа: этап поиска и этап тестирования. На этапе поиска участки последовательно анализируются, причём каждому участку соответствует определённое число кадров. При регистрации фотонного импульса аппаратура переходит к этапу тестирования, в котором в течение заданного числа тестов производится повторный опрос участка. При повторной регистрации фотонного импульса процесс синхронизации (процесс грубой оценки момента приёма фотонного импульса) считается успешно завершённым.

Основная область применения программы – моделирование процесса синхронизации станций системы квантового распределения ключа посредством обнаружения синхроимпульса.

Функциональные возможности программы: задаются исходные параметры передающего и приёмного устройств, линии связи; на выходе рассчитываются вероятностные и энергетические характеристики предлагаемого алгоритма синхронизации.

Лично Миронову Якову Константиновичу принадлежит программная реализация, тестирование и отладка программы.

Миронов Яков Константинович, Румянцев Константин Евгеньевич. Программа моделирования этапа тестирования подсистемы синхронизации системы квантового распределения ключа при разбиении волоконно-оптической линии на участки с убывающей длиной. Свидетельство о государственной регистрации программы для ЭВМ. Номер свидетельства: RU 2022615010. Патентное ведомство: Россия. Год публикации: 2022. Номер заявки: 2022614701. Дата регистрации: 29.03.2022. Язык программирования: MATLAB. Объем: 33 КБ. Правообладатели: федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет».

Программа предназначена для оценки методом имитационного моделирования характеристик этапа тестирования алгоритма синхронизации станций системы квантового распределения ключа при разбиении волоконно-оптической линии на участки с убывающей длиной.

Алгоритм синхронизации станций системы квантового распределения ключа включает поиск фотонного импульса, который осуществляется в два этапа: этап поиска и этап тестирования. Этап поиска состоит в последовательном анализе участков волоконно-оптической линии на предмет регистрации фотонного импульса. При регистрации фотонного импульса аппаратура переходит к этапу тестирования, в течение которого производится повторный опрос предположительно сигнального участка. В случае повторной регистрации фотонного импульса на этапе тестирования процесс грубой оценки момента приёма фотонного импульса считается завершённым.

Основная область применения программы – моделирование этапа тестирования алгоритма синхронизации станций системы квантового распределения ключа.

Функциональные возможности программы: задаются исходные параметры передающего и приёмного устройств, линии связи; на выходе рассчитываются вероятностные и временные характеристики этапа тестирования предлагаемого алгоритма синхронизации.

Лично Миронову Якову Константиновичу принадлежит программная реализация, тестирование и отладка программы.

Научный руководитель, д.т.н., профессор

К.Е. Румянцев

Доцент кафедры ИБТКС

С.Л. Балабаев

Доцент кафедры ИБТКС

А.П. Плёткин

УТВЕРЖДАЮ

Директор Института
компьютерных технологий
и информационной безопасности



Г. Е. Веселов

« 11 » января 2023 г.

Акт внедрения результатов диссертационной работы

Результаты диссертационных исследований соискателя кафедры ИБТКС Миронова Якова Константиновича, посвящённые разработке алгоритма синхронизации станций автокомпенсационной волоконно-оптической системы квантового распределения ключа (КРК) на однофотонном лавинном фотодиоде с разбиением временного кадра на интервалы, использованы при выполнении вузом гранта РФФИ № 20-37-90040:

Разработан новый двухэтапный алгоритм временной синхронизации приёмопередающей и кодирующей станций системы КРК, позволяющий увеличить протяжённость волоконно-оптической линии связи (ВОЛС) благодаря разбиению ВОЛС на участки с убывающей длиной при сохранении энергетической скрытности синхронизации и обеспечивающий вероятность ошибки синхронизации не выше требуемого значения. Впервые получены аналитические выражения для расчёта вероятностных, временных и энергетических характеристик синхронизации согласно предложенному алгоритму при произвольном количестве участков, кадров и тестов. Предложена структура подсистемы синхронизации, реализующая разработанный алгоритм синхронизации, обеспечивающий повышенную безопасность и гарантию увеличения протяжённости ВОЛС.

Результаты диссертационных исследований использованы при написании и публикации статей в сборниках и журналах всероссийского и международного уровней при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90040:

1. Предложена методика разбиения ВОЛС на участки с убывающей длиной в системе КРК. Отличительной особенностью предлагаемой методики является обеспечение требуемой вероятности ошибки синхронизации. Отмечено, что увеличение требуемого числа участков обратно пропорционально снижению вероятности ошибки синхронизации при фиксированном разнесении станций. Определена связь между вероятностью ошибки синхронизации и разнесением станций. С ростом частоты генерации импульсов темнового тока (ИТТ) при заданном значении вероятности ошибки синхронизации протяжённость ВОЛС значительно сокращается. Благодаря постоянству отношения средних чисел фотонов и ИТТ на верхних границах

участков гарантируется вероятность ошибки синхронизации не хуже заданного значения в пределах всей ВОЛС.

Y. K. Mironov, K. E. Rumyantsev. Providing the Required Probability of Synchronization Error When Splitting a Fiber-Optic Line into Sections with Decreasing Length in a Quantum Key Distribution System. Proceedings - 2021 3rd International Conference on System Reliability and Safety Engineering, SRSE, 2022, с. 145-149. DOI: 10.1109/SRSE54209.2021.00032.

Материал апробирован на международной конференции «The 3rd International Conference on System Reliability and Safety Engineering» (SRSE 2021), 26-28 ноября 2021 года, Харбин, Китай.

2. Сформулирован принцип построения двухэтапного алгоритма синхронизации в системе КРК с разбиением ВОЛС на участки с убывающей длиной. Проведён анализ параметров предлагаемого алгоритма. Определены формулы для расчёта временных затрат на процесс синхронизации как для случая успешного тестирования, так и при ошибке тестирования. Дана оценка времени анализа участка ВОЛС, где за допустимое время не обеспечена синхронизация станций системы КРК. Установлены вероятностные характеристики двухэтапного временного алгоритма синхронизации при отсутствии априорной информации о расстоянии между станциями.

Y. Mironov, P. Mironova, K. Rumyantsev. Characteristics of a two-stage synchronization algorithm in the system of quantum key distribution with dividing a fiber-optic line into sections with decreasing length. ACM International Conference Proceeding Series, 2020, paper №3433596, с. 1-5. DOI: 10.1145/3433174.3433595.

Материал апробирован на международной конференции 13th International Conference on Security of Information and Networks (SIN 2020), 4-7 ноября 2020 года, Стамбул, Турция.

3. Предложена методика расчёта среднего времени вхождения в синхронизм станций системы КРК с последовательным опросом участков ВОЛС с убывающей длиной. Построена диаграмма состояний и переходов для последовательного поиска фотонного импульса. Получены аналитические выражения для нахождения вероятности обнаружения фотонного импульса, среднего числа шагов для вхождения в синхронизм станций, дисперсии числа шагов и среднего времени вхождения в связь. Отмечено, что при разбиении ВОЛС на участки с убывающей длиной, уровень ИТТ значительно уменьшается от участка к участку. Последнее позволяет уменьшить вероятность ложных срабатываний фотодетектора. Анализ полученных результатов показал, что время вхождения в синхронизм для предложенного алгоритма в 3 раза меньше времени, необходимого для вхождения в связь станций в случае алгоритма-аналога. Полученные результаты указывают на возможность увеличения протяженности ВОЛС при обеспечении значения вероятности ошибки синхронизации на уровне 0,01.

Y. K. Mironov, P. D. Mironova, K. E. Rumyantsev. Methodology for calculating the average time of entry into synchronism of stations of the system of quantum key distribution with sequential polling of fiber-optic line sections with

decreasing length by the graphic-analytical method. E3S Web of Conferences, Volume 224, с. 1-9. DOI: 10.1051/e3sconf/202022401032.

4. Предложен алгоритм синхронизации станций системы КРК с разбиением ВОЛС на участки с убывающей длиной. Рассмотрен принцип работы данного алгоритма, перспективы его применения. Установлено, что с ростом номера участка время анализа последнего уменьшается, следовательно, наблюдается снижение среднего числа ИТТ, что повышает вероятность успешной синхронизации системы в целом. Благодаря тому, что время между тестированиями превышает время восстановления однофотонного лавинного фотодиода, предлагаемый алгоритм обеспечивает снижение времени вхождения в синхронизм.

Я. К. Миронов. Алгоритм синхронизации станций автокомпенсационной волоконно-оптической системы квантового распределения ключа с разбиением волоконно-оптической линии на участки с убывающей длиной. Материалы I Всероссийской научно-практической конференции. Грозный, 2021 год, с. 94-98. DOI: 10.36684/38-2021-1-94-98.

Материал апробирован на I Всероссийской Научно-Практической Конференции «Digital Era», 26 марта 2021 г., г. Грозный.

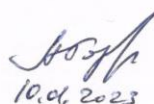
Научный руководитель, д.т.н., профессор  К. Е. Румянцев

Доцент кафедры ИБТКС



С. Л. Балабаев

Доцент кафедры ИБТКС


10.01.2023

А. В. Горбунов