МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет информационных технологий и электроники (наименование)

Кафедра «Нано- и микроэлектроника» (наименование)

Направление подготовки 11.04.04. «Электроника и наноэлектроника» (код и наименование)

Магистерская программа Нано- и микроэлектроника (наименование)

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему

«Разработка методов и подходов совместной передачи классических оптических импульсов и квантовых состояний»

(тем магистерской работы)

Студент 22ПДм1 (номер группы) — 01.06.2024 (подпись, дата) — Филиппов А.В. (фамилия, инициалы)

Научный руководитель к.т.н., доцент, ПГУ (должность, наименование организации) — 03.06.2024 (подпись, дата) — Карманов А.А. (фамилия, инициалы)

Рецензент к.т.н., с.н.с., АО «НИИФИ» (должность, наименование организации) — 06.06.2024 (подпись, дата) — Тюрин М.В. (фамилия, инициалы)

Нормоконтролер старший преподаватель, ПГУ (должность, наименование организации) — 05.06.24 (подпись, дата) — Рыжова Т.Н. (фамилия, инициалы)

Работа допущена к защите в ГЭК (протокол заседания кафедры от 10.06.24 № 10)

Заведующий кафедрой НиМЭ

д.т.н., ПГУ (должность, наименование организации) — 10.06.24 (подпись, дата) — Пронин И.А. (фамилия, инициалы)

Работа защищена с оценкой отл. (протокол заседания ГЭК от 26.06.24 № 10)

Секретарь ГЭК

к.т.н., доцент, ПГУ (должность, наименование организации) — 26.06.24 (подпись, дата) — Вольсков А.А. (фамилия, инициалы)

Пенза, 2024

РЕФЕРАТ

Пояснительная записка выпускной квалификационной работы содержит 85 страниц машинописного текста, включает 21 рисунок, 7 таблиц, 11 формул, список используемых источников из 51 наименований и4 приложения.

Ключевые слова: квантовое распределение ключей, квантовый канал, квантовое состояние, одиночный фотон, многофотонный оптический импульс, классический канал, волоконно-оптическая линия связи, совместная передача, мультиплексирование оптического излучения по длине волны, детектор одиночных фотонов, однофотонный лавинный фотодиод, экономическая эффективность исследования.

Цель работы – сформировать подходы и методы использования существующей инфраструктуры волоконно-оптических сетей связи для совместной передачи классических оптических сигналов и однофотонных квантовых состояний при применение адаптированного детектора одиночных фотонов в аппаратуре квантового распределения ключей (КРК).

Актуальность работы обусловленавысочайшим уровнем информационной безопасности, предоставляемой аппаратурой КРК. Экономически выгодно эксплуатировать аппаратуру КРК на существующей инфраструктуре волоконных сетей, однако на сегодняшний день её использование ограничено высоким уровнем помех при передачи классических сигналов совместно с квантовыми состояниями. Адаптация детектора одиночных фотонов (ДОФ) из состава аппаратуры КРК позволит использовать существующие оптические линии связи для распределения квантовых ключей.

Предмет исследования – технический концепт ДОФ с блочной архитектурой, адаптированный к работе в составе аппаратуры КРК при совмещении классических и квантовых каналов в одном оптическом волокне.

Разработанный концепт ДОФ имеет технические характеристики на уровне лучших аналогов и удовлетворяет требованиям для работы на инфраструктуре существующих оптических линий связи.

СОДЕРЖАНИЕ

Введение 4
1 Теоретические основы совместной передачи классических и квантовых сигналов в одном волокне 7
1.1 Анализ источников по совместной передаче классических и квантовых сигналов в одном оптическом волокне 7
1.2 Подходы и методы эффективной совместной передачи квантовых и информационных оптических сигналов в одном оптическом волокне. 11
1.3 Адаптация аппаратуры КРК 14
1.4 Тактико-технические характеристики ДОФ 17
1.5 Выбор типа чувствительного элемента ДОФ 18
1.6 Описание принципов работы ДОФ на основе ОЛФД 23
1.7 Адаптация ДОФ к работе в общих оптических сетях 31
2 Экспериментальная работа по моделированию совместной передачи классических и квантовых сигналов в одном волокне 36
2.1 Структурная схема адаптированного ДОФ 36
2.2 Параметрыконфигурации ДОФ 43
2.3 Алгоритм работы ДОФ. 44
2.4 Обработка и передача результатов измерения 46
3 Расчет экономической эффективности 49
Заключение 57
Списокиспользованныхисточников 59
Приложение А. Задание на выпускную квалификационную работу 63
Приложение Б. Публикации 65
Приложение В. Антиплагиат 68
Приложение Г. Презентация 71

ВВЕДЕНИЕ

Квантовые коммуникации являются одним из ведущих направлений развития научных изысканий. Наибольших успехов квантовые коммуникации достигли в области квантового распределения ключей (КРК). Технология КРК востребована в задачах информационной безопасности, особенно в условиях многократно возросшего количества атак на критическую инфраструктуру. Правительством РФ утверждена дорожная карта развития квантовых коммуникаций до 2030 года.

Технология КРК получила наибольшее распространение на основе оптоволоконных линий, используемых для передачи квантовых сигналов между модулями аппаратуры КРК. Для организации квантового канала оптимально использовать «темное» (свободное) волокно.

Однако в существующих волокно-оптических линий связи (ВОЛС) темные волокна отсутствуют, а прокладка новых ВОЛС требует значительных материальных вложений. Решением данной ситуации является совместная передача квантовых сигналов аппаратуры КРК и классических информационных сигналов в одном оптическом волокне на основе мультиплексирования с разделением по длине волны.

При совместной передаче квантовых и классических сигналов наблюдается зашумление квантового канала помехами от работы мощных классических каналов, ограничивающая предельную дальность (максимальную длину оптического волокна) между модулями аппаратуры КРК. Подбор режимов работы квантовых и классических каналов позволяет достигнуть оптимальных значений характеристик работы аппаратуры КРК в общей ВОЛС.

С другой стороны обобщение процессов распространения излучения в оптическом волокне при совместной работе квантовых и классических каналов формулирует специальные требования к структурным элементам аппаратуры КРК. Реализация данных требований в аппаратуре КРК позволяет снизить все негативные стороны зашумления квантового канала.

Основным элементом аппаратуры КРК, наиболее чувствительным к зашумлению квантового канала является детектор одиночных фотонов (ДОФ). Адаптация ДОФ под требования совмещения квантовых и классических каналов раскрывает весь технический и экономический потенциал использования аппаратуры КРК и существующей инфраструктуры ВОЛС.

Цель исследования – подходы совместного использования существующей инфраструктуры ВОЛС для передачи квантовых и классических сигналов в рамках одного оптического волокна при работе аппаратуры КРК с адаптированным детектором одиночных фотонов.

Объект исследования – методы совмещения классических и квантовых каналов в одном оптическом волокне для аппаратуры КРК с адаптированным ДОФ, в том числе – оптические и электрические процессы, происходящие при регистрации оптического излучения с энергией, сопоставимой с энергией одного фотона.

Предмет исследования – технический концепт ДОФ с блочной архитектурой, адаптированный к работе в составе аппаратуры КРК при совмещении классических и квантовых каналов в одном оптическом волокне.

Задачи исследования:

– определить основные подходы к совместному использованию существующей инфраструктуры оптических транспортных сетей для организации каналов связи аппаратуры квантового распределения ключей;

– разработать методы организации совместной передачи классических и квантовых сигналов в рамках одного оптического волокна на основе мультиплексирования с разделением по длине волны оптических сигналов;

– определить требования к структурным элементам аппаратуры КРК, обусловленные фактом объединения классических и квантовых сигналов в одном оптическом волокне;

– выполнить адаптацию структурных элементов аппаратуры КРК, обеспечивающих улучшенные тактико-технические характеристики при объединения классических и квантовых сигналов в одном оптическом волокне.

Методологические и теоретические основы исследования – поиск, систематизация и анализ открытых публикаций за последние 10 лет по теме диссертации.

Методы исследования – в процессе выполнения исследования, описания его результатов использовались теоретические и математические методы познания.

Теоретическая и практическая значимость результатов. Результаты данной работы представляют развитие в методах и подходах совместной передачи классических оптических импульсов и квантовых состояний. Акцент сделан на технические решения, обеспечивающие адаптацию аппаратуры КРК к её использованию на инфраструктуре существующих оптических транспортных сетей. Для адаптации аппаратуры КРК к совместной работе на инфраструктуре существующих оптических транспортных сетей особо выделен детектор одиночных фотонов (ДОФ). Модернизация ДОФ позволит уменьшить негативные последствия использования засвеченных оптических волокон для передачи квантовых состояний. Сформулированы дополнительные требования к ДОФ.

Апробация результатов диссертации. Материалы исследования, изложенные в квалификационной работе, докладывались на:

– первый всероссийский форум «Доверенные квантовые технологии и коммуникации» (КВАНТ’2023);

– второй всероссийский форум «Доверенные квантовые технологии и коммуникации» (КВАНТ’2024);

– научно-практическая конференция «Технологическая независимость и информационная безопасность: от микросхем до систем» (ЦИФРА-2024).

Публикации. Основными публикациями являются (ПРИЛОЖЕНИЕ Б):

– патент RU 2 792 414 C1 «Способ передачи информации между конечными узлами связи через промежуточные узлы без перешифрования»

– патент RU 2 817 659 C2 «Динамическая система формирования и распределения ключей без компрометации ключевой информации».

1 Теоретические основы совместной передачи классических и квантовых сигналов в одном волокне

При освещении задачи совместной передачи классических и квантовых сигналов в одном волокне рассматриваются такие теоретические вопросы как:

– анализ существующих подходов к решению задачи совместной передачи;

– выбор оптимальных методов и подходов совместной передачи оптических сигналов;

– выявление и формулирование общих требований к аппаратуре КРК при её использовании на совместных оптических линиях связи;

– формулирование требований к структурным блокам аппаратуры КРК;

– разработка предложений по адаптации структурных модулей аппаратуры КРК для возможности работы на совместных оптических линиях связи.

1.1 Анализ источников по совместной передаче классических и квантовых сигналов в одном оптическом волокне

Первая схема мультиплексирования с разделением по длине волны квантовых каналов (КК) систем КРК и классических информационных каналов в одном оптическом волокне была предложена Таунсендом в 1997 году [1]. В рамках данной работы впервые было предложено использовать спектральное уплотнение, при этом квантовому каналу соответствовала длина волны 1310 нм, а классические данные передавались на длине волны 1550 нм. Передатчик (Алиса) и приемник (Боб) были связаны стандартным телекоммуникационным оптоволокном длиной 28 км. Предложенный Таунсендом подход продемонстрировал принципиальную возможность передачи квантовых состояний и классической информации в одном оптическом оптоволокне, при этом было показано что уровень квантовой ошибки *QBER* зависит от мощности лазерного излучения, соответствующей информационному каналу.

Впоследствии [2-4] было предложено для уменьшения шума от классических каналов, соответствующих *C*-диапазону (*C-band*) прозрачности оптоволокна (1530-1565 нм), распределять квантовые состояния на длинах волн, отвечающих *O*-диапазону (*O-band*) прозрачности (1260-1360 нм). Однако, как известно, оптическое поглощение в *O*-диапазоне существенно выше, чем в *C*-диапазоне [4], что сильно ограничивает максимальную дальность передачи квантовых состояний.

В рамках работы [5] была впервые продемонстрирована совместная передача квантовых каналов аппаратуры КРК и 1 Гбит/с информационных каналов в одном оптическом волокне при использовании *L*-диапазона прозрачности оптоволокна.

По данным работы [5] однопроходные оптоволоконные системы КРК с фазовым кодированием ослабленных лазерных импульсов могут быть эффективно объединены с известными технологиями плотного спектрального уплотнения при условии ограничения (с помощью перестраиваемых аттенюаторов*VOA*) мощности лазерного излучения, соответствующей информационным каналам. В частности, было показано, что использование в качестве несущей длины волны квантового канала 1551.72 нм и дуплексных классических каналов на 1555.75 и 1553.33 нм обеспечивает выработку и распределение квантовых ключей по протоколу *BB84* на расстояние 41 км со скоростью 2 бит/с. Использование полосовых оптических фильтров позволяет увеличить максимальную длину оптоволокна и/или скорость выработки секретного ключа за счет уменьшения влияния нелинейных эффектов.

Аналогичные результаты получены в работе [9], в рамках которой продемонстрирована возможность квантового распределения ключей для сетей с пропускной способностью 10 Гб/с на базе технологии плотного спектрального уплотнения. Модуль *DWDM* с 8 каналами связи на приемной и передающей стороне использовался для объединения классических информационных каналов, канала синхронизации и квантового канала системы КРК, использующей фазовое кодирование ослабленных лазер импульсов.

По данным работы [9] максимально достигнутая скорость выработки секретного ключа составляла 2.38 Мб/с, 1.17 Мб/с, 177 кб/с и 52 кб/с для линий связи длиной 35, 50, 65 и 70 км соответственно.

Для обеспечения высоких параметров передачи использовались следующие подходы:

1) временная фильтрация сигнала однофотонных детекторов;

2) контроль мощности лазерных импульсов в классических каналах передачи в зависимости от длины линии связи;

3) спектральная фильтрация входящих импульсов, обеспечивающая уменьшение шума от рамановского рассеяния, за счет использования узких полосовых оптических фильтров.

Также значительный интерес представляют результаты работы [11], в которой рассмотрены принципы объединения высокоскоростной системы КРК с высокоскоростными классическими шифраторами. При этом плотное спектральное уплотнение (*DWDM*) используется в высокоскоростной системе передачи данных (*HSE*) для объединения информационных каналов (100 Гб/с на длинах волн 1529.55 и 1529.94 нм), а грубое спектральное уплотнение (*CWDM*) применяется для объединения классических и квантовых каналов. На приемной стороне ослабленные лазерные импульсы, кодирующие квантовые состояния, фильтруются по длине волны с помощью 25 или 100 ГГц спектральных фильтров для уменьшения уровня шума, а соответственно и *QBER*.

Отдельно следует отметить, что использование приемной стороной более узкого спектрального фильтра позволяет увеличить максимальную дистанцию передачи квантового ключа, но на малых расстояниях значительно уменьшает секретный битрейт.

Близкий, по сути, но при этом более широкий подход по объединению информационных и квантовых каналов в одном оптическом волокне изложен в работе [14]. Основная идея данного подхода заключается в использовании

многоядерного оптоволокна (*MCF*) совместно с плотным спектральным уплотнением.

Увеличение мощности классических информационных сигналов приводит к уменьшению скорости выработки секретного ключа с одновременным ростом *QBER* за счет паразитного (создающего шумы) влияния ядер друг на друга. Аналогичная ситуация наблюдается и при увеличении дальности передачи.

Ниже в таблице 1 представлен перечень работ, посвященных совместной передаче квантовых каналов систем КРК и информационных каналов в одном оптическом волокне.

В ней отражены основные результаты экспериментов, включая дальность передачи (L_{max}), используемая длина волны для квантового (λ_q) и информационных (λ_i) каналов, скорость выработки секретного ключа (r_{sec}) и тип оптоволокна.

На основе приведенного выше обзора работ, посвященных вопросам совместной реализации квантовых каналов систем КРК и информационных каналов в одном оптическом волокне, можно сделать заключение, что данная задача имеет решение. Однако необходимо учитывать, что в каждом конкретном случае (модель оборудования КРК, тип оптического волокна) возможно потребуется индивидуальный подход к реализации схемы совместной передачи квантовых и информационных каналов в одном оптическом волокне.

Таблица 1 – Основные результаты экспериментов по совместной передаче квантовых каналов систем КРК и информационных каналов в одном оптическом волокне

Авторы, ссылка на работу, год	L_{max}, км	λ_q, нм	λ_i, нм	r_{sec}, бит/с	Тип оптоволокна
Townsend [1], 1997	28	1300	1591	-	*SMF-28*
Nweke [2], 2005	10	1310	1465-1525	70	*SMF-28*
Runser [3], 2007	50	1310, 1560	1530	-	*SMF-28*
Chapuran [4], 2009	25	1310	*C-band*	10	*SMF-28*
Eraerds [5], 2010	41	1551.72	1553.33 1555.75	7	*SMF-28*
Choi [6], 2010	10	1290	1310, 1550	1300	-
Patel [7], 2012	90	1550	1591-1611	7600	*DSF*
Mora [8], 2012	11	1551	1531. 1571	$2 \cdot 10^5$	*SMF-28*
Patel [9], 2014	25	1548.52	1552.52 1553.33	$4.45 \cdot 10^5$	*DSF*
Kumar [10], 2015	75	1530	1550	500	*SMF-28*
Dynes [11], 2016	101	1547,72	1529.55 1529.94	10 000	-
Wang [12], 2017	80	1310	1550	1000	*SMF-28*
Mao [13], 2018	75	1310	1528-1538	5100	*SMF-28*
Cai [14], 2019	40	1550,39	1551,19 1549,59	10900	*Multicore fiber*
Eriksson [15], 2019	10	1549,5	*C-band*	27200	*SMF-28*

1.2 Подходы и методы эффективной совместной передачи квантовых и информационных оптических сигналов в одном оптическом волокне.

Основные каналы, необходимые для взаимодействия аппаратуры квантового распределения ключей, показаны на рисунке 1.

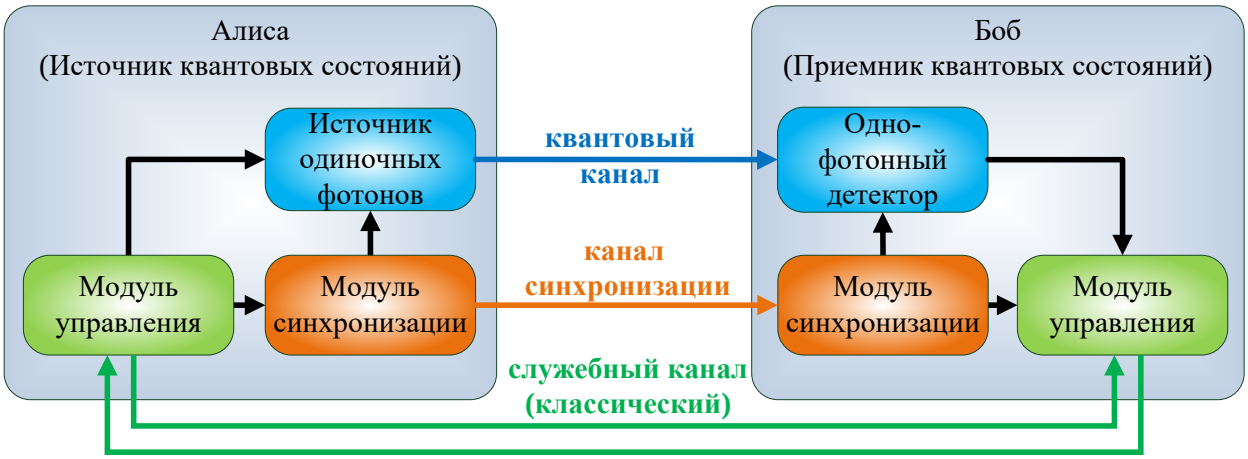


Рисунок 1 – Каналы взаимодействия ККС

Необходимы каналы взаимодействия технических средств ККС:

– квантовый канал;

– канал синхронизации;

– служебный канал.

Квантовый канал предназначен для передачи квантовых состояний. Для организации квантового канала используют выделенное «темное» оптоволокно.

Канал синхронизации используется для временной синхронизации передающей и приемной стороны квантовой системы. Для организации канала синхронизации используют выделенное «темное» оптоволокно.

Служебный канал используется для обмена классической (несекретной) информацией между передающей и приемной стороной аппаратуры КРК в процессе выполнения квантового протокола и последующей процедуре обработки полученной информации. Для организации служебного канала обычно используют сетевой ресурс транспортных сетей связи, учитывая возможность длины квантового канала до 100 км.

При использовании оборудования спектрального уплотнения каналов возможно функциональное объединение квантового, служебного и канала синхронизации в одном оптическом волокне (рисунок 2).

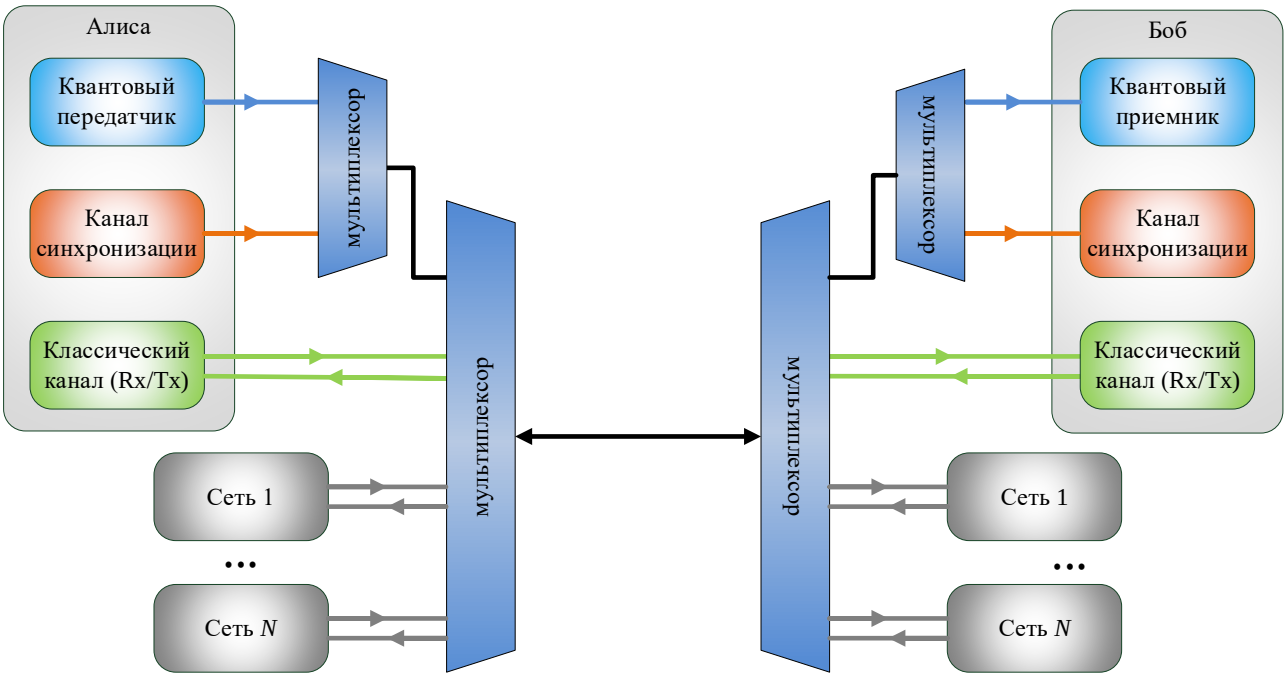


Рисунок 2 – Схема интеграции аппаратуры КРК в оптические сети

В данном схеме имеется несколько конструктивных особенностей, которые используются для поддержания изоляции между квантовыми и классическими каналами.

Во-первых, при совместной передаче сигналов аппаратуры КРК и классических сигналов оптический план канала должен минимизировать шум, генерируемый классическими каналами и нелинейными взаимодействиями с квантовыми сигналами.

В-вторых, должен быть реализован «принцип обхода», т.е. сеть должна позволять квантовым сигналам обходить элементы, которые не совместимы с квантовыми каналами, такие как оптические усилители и непрозрачные узлы, которые преобразуют оптический сигнал в электрический.

В-третьих, архитектура оптических переключателей должна минимизировать оптические потери для квантовых сигналов и не иметь перекрестной связи от классических каналов.

В-четвертых, при демультиплексировании классических и квантовых каналов на приемной стороне должна обеспечиваться их высокая изоляция на уровне 100 дБ, а также дополнительная спектральная фильтрация для устранения иных источников шума.

В-пятых, должно быть реализовано максимальное разнесение рабочих длин волн квантовых и классических сигналов.

1.3 Адаптация аппаратуры КРК

Для адаптации аппаратуры КРК к использованию в общей оптической линии связи совместно с телекоммуникационным оборудованием необходимо:

– определить наиболее критичные структурные элементы аппаратуры квантового распределения ключей, чувствительные к факту объединения классических и квантовых сигналов в одном оптическом волокне;

– разработать предложения по доработке аппаратуры квантового распределения ключей, обеспечивающих улучшенные тактико-технические характеристики при объединения классических и квантовых сигналов в одном оптическом волокне.

Структурная схема аппаратуры КРК приведена на рисунке 3.

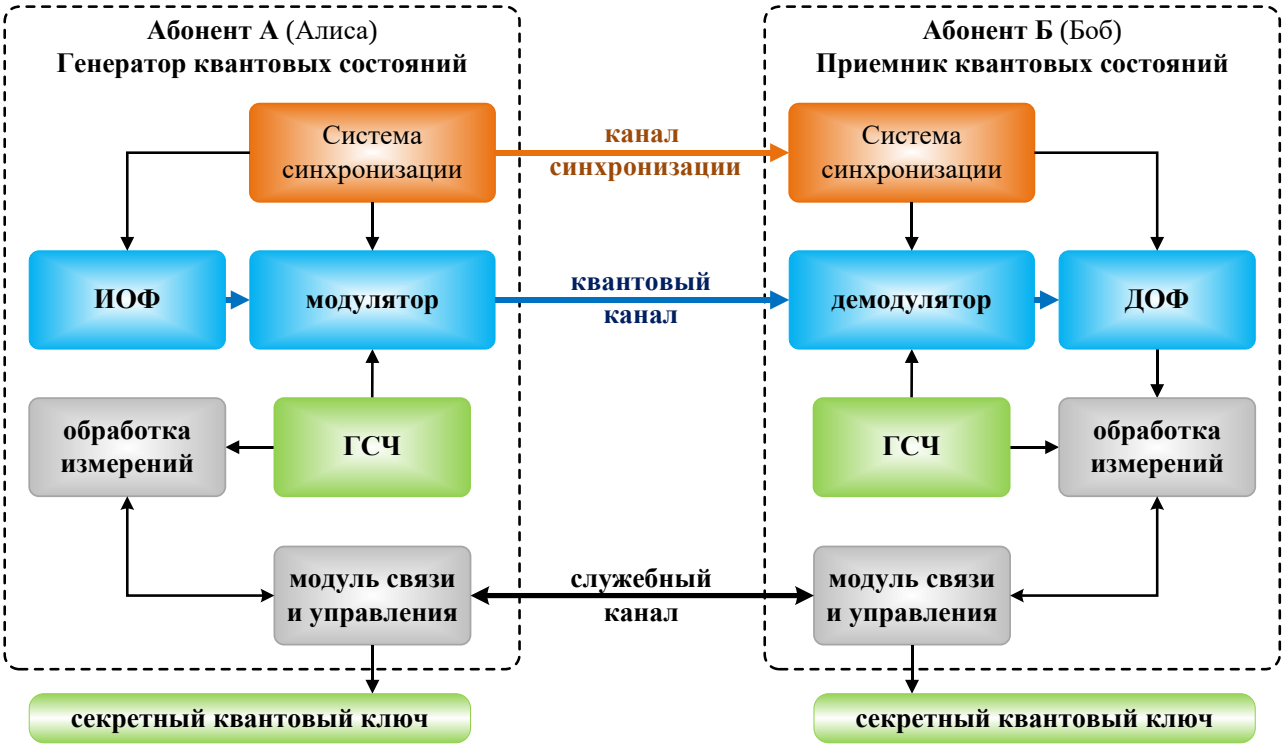


Рисунок 3 – Структурная схема аппаратуры КРК

Начальным и финальным элементами квантового канала как структурного элементом аппаратуры КРК являются источник одиночных фотонов (ИОФ) и детектор одиночных фотонов (ДОФ).

Основные искажения передаваемых квантовых состояний при объединении классического и квантового канала происходят в оптическом волокне, соединяющем приемно-передающие модули аппаратуры КРК, и объясняются генерацией шумовых квантовых состояний из-за нелинейных оптических эффектов при распространении классических сигналов в оптическом волокне.

Мощность (количество) шумовых квантовых состояний обладает следующим свойствами:

– пропорциональна мощности оптического излучения классических каналов;

– равномерно распределена во времени (при условии, что мощность классических каналов постоянна во времени);

– сконцентрирована по нормальному распределению вокруг значений рабочих длин волн классических каналов.

Аппаратура КРК, использующая оптическое волокно для передачи квантовых состояний, может использовать поляризационное или фазовое кодирование квантовых состояний. Нелинейные оптические эффекты в волокне не приводят к искажению модуляции квантовых состояний. А все квантовые ошибки в работе аппаратуры КРК вызваны шумовыми квантовыми состояниями. Учитывая пространственно-временное распределение шумовых квантовых состояний, основные требования предъявляются к ИОФ и ДОФ для возможности работы аппаратуры КРК в общих оптических сетях связи.

1.3.1 Основные требования к источнику одиночных фотонов (ИОФ) для адаптации аппаратуры КРК к работе в общих оптических сетях исходят из особенностей пространственно-временного распределения шумовых квантовых состояний.

Для увеличения вероятности регистрации именно информационного квантового состояния его средняя мощность должна быть больше средней мощности шумовых квантовых состояний в единицу времени. Для этого ИОФ

должен концентрировать энергию при формировании носителя квантового состояния – одиночного фотона – как во времени, так и по длине волны.

Использование высоко когерентных*DFB*-лазеров позволяет сузить ширину спектра оптического излучения до 0,1 нм на уровне -3 дБ, при этом позволяет использовать более узкополосные оптические фильтры без снижения эффективности работы аппаратуры КРК.

Использование коротких оптических импульсов (0,3-0,5 нс) концентрирует энергию в узком временном окне, что позволяет повысить среднюю мощность информационного квантового состояния при сохранении средней энергии квантового состояния.

1.3.2 Основные требования к детектору одиночных фотонов (ДОФ) для адаптации аппаратуры КРК к работе в общих оптических сетях так же исходят из особенностей пространственно-временного распределения шумовых квантовых состояний.

Детектор одиночных фотонов является более сложным техническим устройством по сравнению с ИОФ. ДОФ работает в стробируемом (гейгеровском) режиме, разрешая регистрацию входящего излучения в строго заданные временные окна.

Для увеличения вероятности регистрации именно информационного квантового состояния ДОФ должен «открываться» – быть способным зарегистрировать одиночный фотон – именно в моменты прихода информационного квантового состояния и быть «закрытым» в остальное время – для исключения возможности регистрации шумового квантового состояния.

Таким образом, ДОФ для противодействия шумовым квантовым состояниям должен обладать следующими свойствами:

– работать по управляющему синхроимпульсу, формируемому подсистемой синхронизации аппаратуры КРК;

– физическое временное окно регистрации одиночных фотонов должно быть регулируемым и иметь максимально крутые фронты;

– логическое временное окно регистрации одиночных фотонов должно быть регулируемым;

– иметь защиту от перегрузки по мощности входящего оптического излучения, с регистрацией факта перегрузки.

1.4 Тактико-технические характеристики ДОФ

К основным характеристикам ДОФ относят следующие параметры:

1) *квантовая эффективность* – вероятность регистрации одиночного фотона. Т.е. отношение количества зарегистрированных фотонов к общему числу пришедших фотонов.

Примечание. Если на детектор одновременно приходят несколько фотонов, то вероятность его срабатывания повышается, однако различить количество пришедших фотонов в таком случае невозможно;

2) *частота «темновых» отсчетов* – количество ложных срабатываний детектора в единицу времени в отсутствие входного сигнала. Данная величина является характеристикой собственных шумов детектора;

3) *время восстановления* или «мертвое» время, τ, представляет собой интервал времени, который следует после поглощения фотона, в течение которого детектор не может надежно зарегистрировать последующий фотон. Мертвое время ограничивает максимальную скорость счета детектора;

4) *вероятность возникновения остаточного импульса* (послеимпульса). При срабатывании детектора его чувствительный элемент может находиться в частично-возбужденном состоянии. Частично-возбужденное состояние чувствительного элемента детектора со временем распадается, что в некоторых случаях приводит к ложному срабатыванию детектора при отсутствие входящих фотонов. Вероятность появления остаточного импульса рассчитывается как количество возникших остаточных импульсов по отношению к ранее обнаруженным фотонам за определённый временной отрезок.

5) *временной джиттер* –это изменение временного интервала между поглощением фотона и генерацией выходного электрического импульса детектора. Дрожание временного джиттера обуславливается временем прихода оптического импульса относительно внутренней частоты обработки состояний элементов детектора.

С учетом анализа технических характеристик коммерческих ДОФ адаптируемый к работе на общих оптических сетях ДОФ должен обладать характеристиками, не хуже, чем приведенные в таблице 2.

Таблица 2 – Обобщенные технические характеристики ДОФ

Наименование параметра	Значение
Квантовая эффективность регистрации одиночных фотонов, не менее, %	25
Частота темновых отсчетов (при квантовой эффективности 10%), за секунду, не более, шт.	1000
«Мертвое» время после срабатывания, настраивается, мкс	1..100
Вероятность послеимпульса, не более, %	1
Частота стробирования, не менее, МГЦ	100
Эффективная ширина строба, нс	0,5..5
Разрешение по времени, не более, пс	1000

1.5 Выбор типа чувствительного элемента ДОФ

В данном пункте анализируются существующие физические устройства регистрации оптического излучения, обладающие чувствительностью реагировать на одиночные фотоны

ДОФ можно реализовать на основе следующих однофотонных чувствительных элементов:

1) фотоэлектронные умножители (ФЭУ);

2) однофотонныелавинныефотодиоды (*Single photon avalanche diode, SPAD*);

3) кремниевые фотоумножители (*SiPM*);

4) детекторы на основе сверхпроводящих нанопроволок (*Superconducting Nanowire Single Photon Detector, SNSPD*);

5) сверхпроводящие болометры (*TES*);

6) фотодетекторы с квантовыми точками.

1.5.1 Фотоумножители (ФЭУ) имеют большую активную площадь (диаметр >10 мм) и охватывают спектральный диапазон 115–1700 нм, но с большими вариациями характеристик. Базовый ФЭУ состоит из вакуумной трубки с фотокатодом для поглощения света, из которого за счет фотоэлектрического эффекта высвобождаются электроны (энергия падающего фотона должна превышать работу выхода материала фотокатода). Затем этот фототок с одним или несколькими электронами умножается в каскаде из динодов – ряда электродов, каждый из которых смещен в большем напряжением, чем предыдущий, – создавая макроскопический импульс тока из $>10^6$ электронов. Традиционные ФЭУ требуют больших рабочих напряжений порядка киловольт и обладают низкой квантовой эффективностью на уровне 2% на длине волны 1550 нм.

1.5.2 Однофотонный лавинный фотодиод (ОЛФД) –является твердотельным полупроводниковым устройством, в основе которого лежит структура лавинного фотодиода (*p–n* или *p–i–n* переход). Диод смещен в обратном направлении выше напряжения пробоя (работа в режиме Гейгера). Носители, генерируемые при поглощениии фотонов, подвергаются лавинному усилению, вызывая макроскопический пробой диодного перехода. Чтобы использовать этот эффект в практическом устройстве, необходимо иметь возможность останавливать лавину с помощью схемы гашения.

Новое поколение ОЛФД – это планарные структуры с неглубоким переходом диаметром 50 мкм, для которых требуется довольно низкое рабочее

напряжение. Джиттер составляет менее 40 пс на полувысоте. Структура ОЛФД показана на рисунке 4.

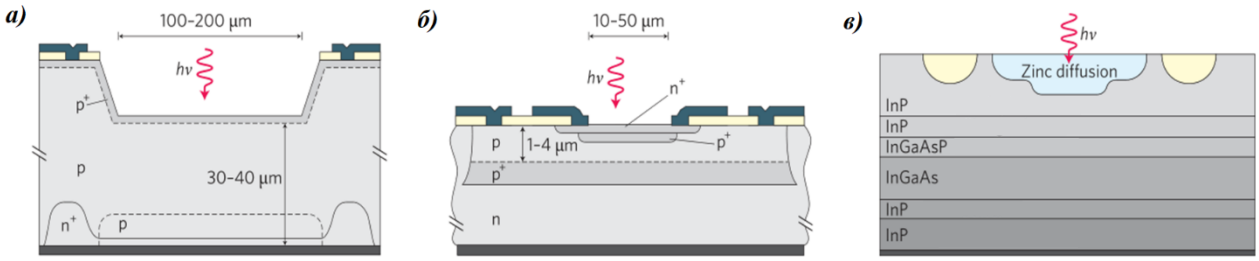


Рисунок 4 – Структура однофотонного ЛФД

ОЛФД различают на следующие типы:

– кремниевые ОЛФДс толстым переходом (рисунок 4 а). Структура устройства оптимизирована для высокой эффективности обнаружения и низкого количества темновых импульсов;

– планарный кремниевыйОЛФД с неглубоким переходом (рисунок 4 б). Структура устройстваоптимизирована для низкого временного джиттера, требующего низкого напряжения смещения;

– ОЛФД со структурой InGaAs/InP (рисунок 4 в), в которой использование полупроводника с меньшей шириной запрещенной зоны расширяет однофотонную чувствительность на телекоммуникационных длинах волн.

Наилучшие результаты были достигнуты с областью поглощения InGaAs и умножающим слоем InP, что обеспечивает однофотонную чувствительность в диапазоне длин волн 1000–1600 нм и пиковую эффективность ~ 20% на 1550 нм [20–21].

ОЛФД на InGaAs обычно работают в гейгеровском стробированном режиме – устройство в состоянии покоя смещается ниже напряжения пробоя, затем подается короткий (~ 1 нс) импульс, совпадающий с ожидаемым прибытием фотона.

Темновую скорость счета можно уменьшить путем охлаждения до ~200 К, но это снижение температуры увеличивает вероятность постимпульсов,

вызывая длительное мертвое время детектора около 10 мкс и снижая максимальнюу скорость счета.

1.5.3 Кремниевый фотоумножитель – массив пикселей ОЛФД, которые считываются параллельно – может реализовать чрезвычайно высокую скорость счета (~ 400 МГц) и разрешение по количеству фотонов, но страдает от повышенного количества темновых отсчетов [19].

Чтобы расширить характеристики ОЛФД до длин волн телекоммуникаций (λ = 1310 нм и 1550 нм), используются полупроводниковые материалы с меньшей шириной запрещенной зоны, такие как Ge и InGaAs.

1.5.4 Однофотонные детекторы со сверхпроводящими нанопроволоками (*SNSPD*) [27-28] обеспечивают чувствительность к одиночным фотонам в диапазоне длин волн от видимого до среднего инфракрасного, низкое значение темнового счета, короткое время восстановления и низкий временной джиттер.

Сам детекторный элемент представляет собой нанопроволоку шириной 100 нм, рисунок которой с помощью электронно-лучевой литографии нанесен на ультратонкую сверхпроводящую пленку из нитрида ниобия [28]. Он работает в диапазоне температур 1,5–4 К, что значительно ниже температуры сверхпроводящего перехода пленки нитрида ниобия. Этот материал выбран из-за его исключительной светочувствительности [28]. Сверхпроводящий провод смещается чуть ниже критического тока, который является точкой, в которой провод становится резистивным. Когда фотон попадает на провод, образуется локальная резистивная горячая точка, которая возмущает распределение тока и, таким образом, вызывает быстрый импульс напряжения [27], который затем можно усилить и измерить.

Эффективность обнаружения и скорость темнового счета зависят от точки смещения, при этом скорость темнового счета возрастает более резко вблизи критического тока.

Современные устройства состоят из «меандровой проволоки»[29], которая покрывает площадь до 20 мкм × 20 мкм [30] для достижения высокой

эффективности связи между нанопроволокой и одномодовым оптическим волокном.

1.5.5 Другой новый класс устройств использует улавливание заряда в дефектах для обнаружения одиночных фотонов. Полупроводниковые гетероструктуры на основе соединений *iii–v* формируют базовую архитектуру устройства: для захвата используются либо квантовые точки (КТ), внедренные в материал [36–37], либо собственные дефекты [38].

КТ предпочтительнее, поскольку их можно контролируемо размещать внутри гетероструктуры, чтобы максимизировать внутреннюю эффективность и однородность сигнала.

Были реализованы две основные схемы обнаружения. Первая основана на фотопроводящем механизме усиления, который включает захват заряда в дефект или слой квантовых точек, что изменяет проводимость в структуре полевого транзистора [38]. Эти типы устройств работали при скоростях счета до 400 кГц [39], а высокая эффективность до 68% была продемонстрирована на 805 нм [36]. Также было продемонстрировано разрешение до трех фотонов в таких устройствах [37]. Вторая схема основана на фотопоглощении в КТ, что изменяет вероятность туннелирования в резонансной туннельной диодной структуре [40].

1.5.6 Обобщенные характеристики однофотонных чувствительных элементов приведены в таблице 3.

Таблица 3 – Характеристики детекторов

Тип детектора	Рабочая температура, К	Квантовая эффектив-ность	Темно-вой счет	Максимальная частота дискретизации	Много-фотонное разрешение
ФЭУ (ближний ИК)	300	40% при 500 нм	100 Гц	10 МГц	+
ФЭУ (ИК)	200	2% при 1,550 нм	200 кГц	10 МГц	+
Si ОЛФД	250	65% при 650 нм	25 Гц	10 МГц	-
InGaAs ОЛФД	240	10% при 1,550 нм	16 кГц	100 МГц	+

SNSPD	3	0.7% при 1,550 нм	10 Гц	100 МГц	-
SNSPD	1,5	57% при 1,550 нм	-	1 ГГц	-
Квантовые точки	4	12% при 550 нм	2 × 10–3 Гц	250 кГц	-

1.5.7 На основе анализа данных таблицы наиболее выгодным решением будет использование однотонного лавинного фотодиода в качестве регистрирующего элемента ДОФ для телекоммуникационных длин волн 1200-1700 нм.

Использование ОЛФД позволит создать малогабаритный ДОФ с хорошими техническими характеристиками.

1.6 Описание принципов работы ДОФ на основе ОЛФД

Структурная схема и описание детектора одиночных фотонов (ДОФ) на основе однофотонного лавинного фотодиода (ОЛФД), взятая за основу при разработке адаптированного ДОФ, приведена на рисунке 5 [45].

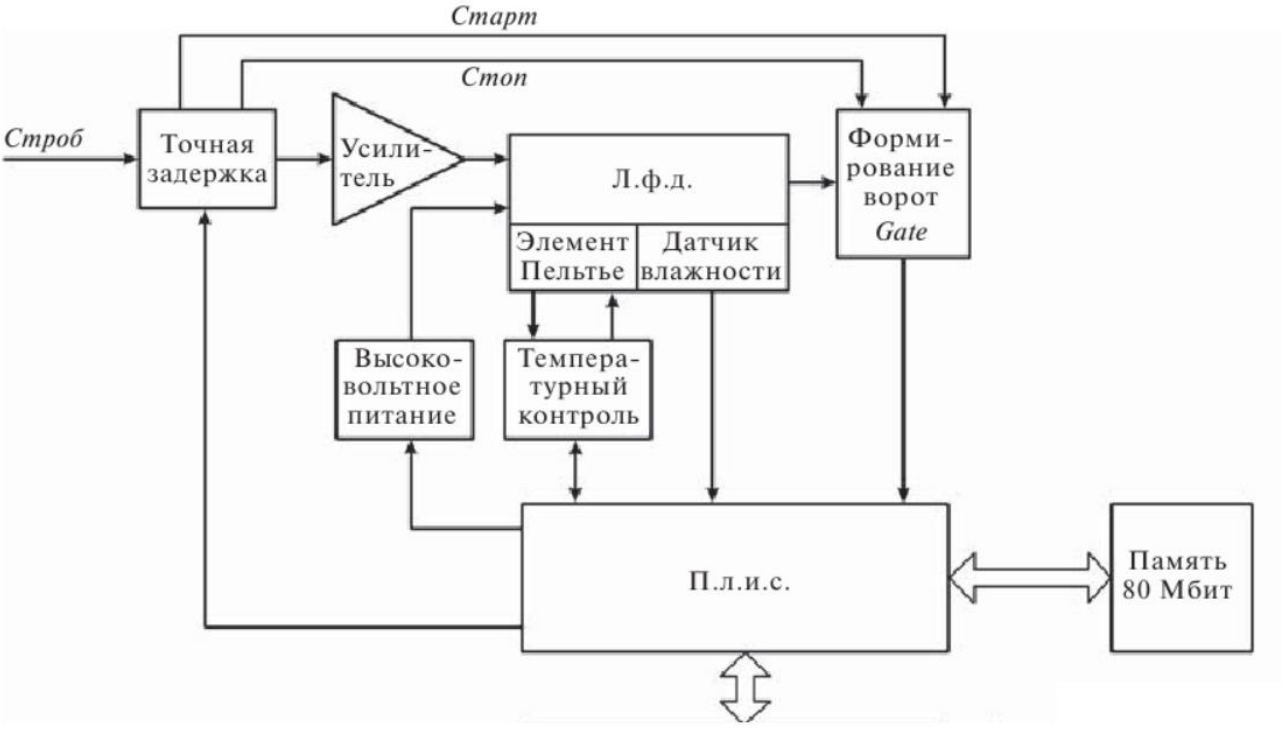


Рисунок 5 – Базовая структурная схема ДОФ

Работой всего ДОФ управляет ПЛИС, содержащая в своем составе ядро процессора, так называемая система на кристалле. Для сохранения результатов

измерения к ПЛИС подключен модуль памяти. За поддержания оптимальных параметров работы ОЛФД отвечают драйвер температурного контроля и драйвер источника высоковольтного напряжения. Временной синхронизацией совместной работой по формированию строба измерения и обработки результатов измерения отвечает подсистема синхронизации, состоящая из управляемых линий задержек и логического блока формирователя временных ворот (*gate*). Структура подсистемы синхронизации (основная часть) приведена на рисунке 6[45].

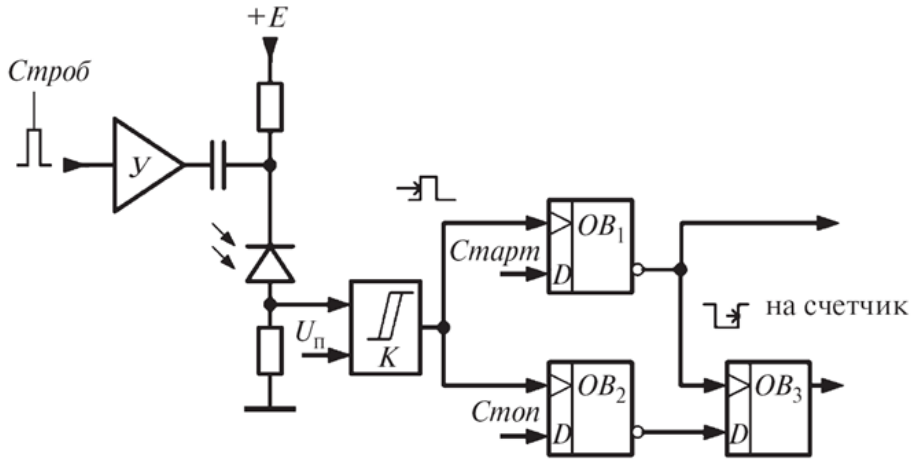


Рисунок 6 – Упрощенная схема прохождения сигнал ОЛФД

В случае возникновения пробоя ОЛФД (попадание фотона или темновой шум) возникает ток через него, что приводит к увеличению напряжения на резисторе, подключенном к аноду. Напряжение с резистора попадает на вход компаратора *К* (на инверсный вход подается опорное напряжение). Сигнал, сформированный компаратором (его длительность зависит от длительности строб-сигнала и момента времени, в который произошло срабатываниеОЛФД), поступает на *С*-вход триггеров ОВ1 и ОВ2, выполняющих роль одновибраторов. На *D*-вход триггеров подаются импульсы СТАРТ и СТОП, определяющие временное окно (*Gate*).

Возможны три варианта времени появления импульса ОЛФДна выходе компаратора*К* относительно временных ворот. Временные диаграммы данных событий показаны на рисунке 7.

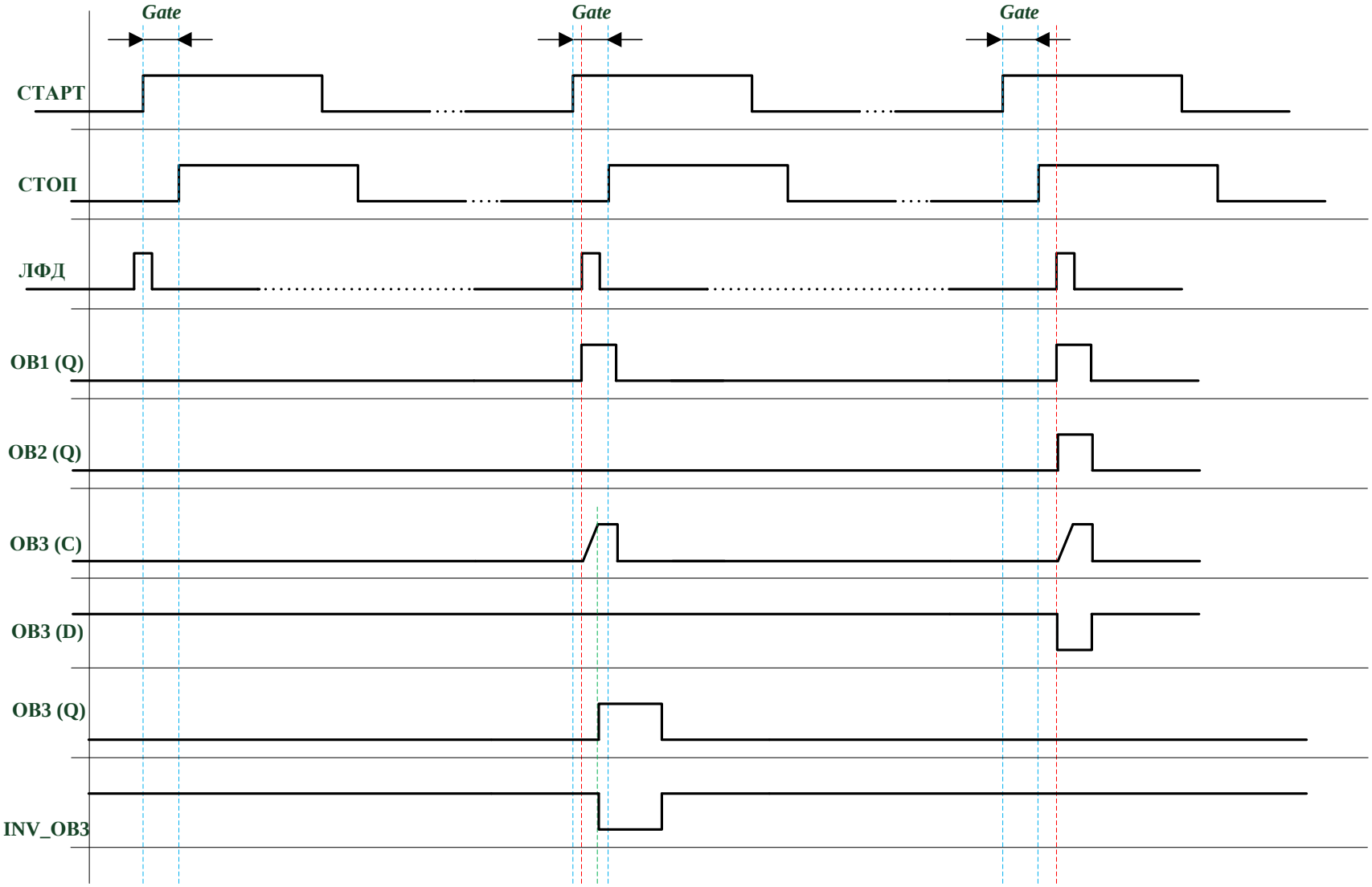


Рисунок 7 – Временная диаграмма срабатывания ОЛФД относительно временных ворот

Первый вариант. Импульс ОЛФД (его передний фронт) появляется до импульсов СТАРТ и СТОП (рисунок 7, первая вертикаль). В этом случае появление импульса срабатывания ОЛФД на выходе компаратора не приводит к появлению импульса на выходе логического блока ОВ1-ОВ3.

Второй вариант. Импульс ОЛФД (его передний фронт) появляется между началами импульсов СТАРТ и СТОП, т.е. находится в рабочем временном окне (*Gate*). В этом случае одновибратор ОВ1 по сигналу сигнал СТАРТ формирует импульс (длительность определяется значением *RC*-цепочки в лини обратной связи, на рисунке не показана), а одновибратор ОВ2 по сигналу СТОП не изменяет своего состояния. В результате на вход «*C*» одновибратора ОВ3 подается импульс, что при отсутствии сигнала на входе «*D*», приводит к появлению импульса на выходе «*Q*» одновибратора ОВ3, то есть всего логического блока ОВ1-ОВ3. Данный сигнал (импульс) говорит о срабатывании ОЛФД в заданных временных воротах.

Третий вариант. Импульс ОЛФД (его передний фронт) появляется после начала импульсов СТАРТ и СТОП. В этом случае одновибратор ОВ1 по сигналу СТАРТ формирует импульс на выходе «*Q*» и одновибратор ОВ2 по сигналу СТОП также формирует импульс на своем выходе «*Q*». Время появления импульсов на выходе ОВ1 и ОВ2 одинаковое (т.к. они синхронизированы управляющим сигналом от компаратора). Полученные импульсы подаются на входы «*C*» и «*D*» одновибратора ОВ3. В отличие от второго варианта, присутствие сигнала на входе «*D*» одновибратора ОВ3, запрещает появление импульса на его выходе.

На вход «*D*» одновибратора ОВ3 поступает сигнал с инверсного выхода одновибратора ОВ2, синхронизированного сигналом СТОП по входу «*D*». На вход «*C*» одновибратора ОВ3 поступает сигнал с прямого выхода одновибратора ОВ1, синхронизированных сигналом СТАРТ (с небольшой задержкой, определяемой *RC*-цепочкой на входе). В результате сигнал (импульс) на прямом выходе ОВ3 появляется только во втором варианте, если

срабатывание ОЛФД произошло между началом импульса СТАРТ и началом импульса СТОП.

ОЛФД могут включатьсяв линейном режиме с напряжением смещения ниже напряжения пробоя (рисунок 8, левая диаграмма). В таком режиме ток через детектор пропорционален мощности оптического излучения на входеОЛФД (так работают телекоммуникационные лавинные фотодетекторы). В режиме счета фотонов (или в гейгеровском режиме) на детектор подается смещение выше напряжения пробоя (рисунок 8, правая диаграмма). Пробой может вызвать случайно сорвавшийся электрон (и это будет темновой отсчет) или электрон выбитый фотоном входящего оптического излучения.

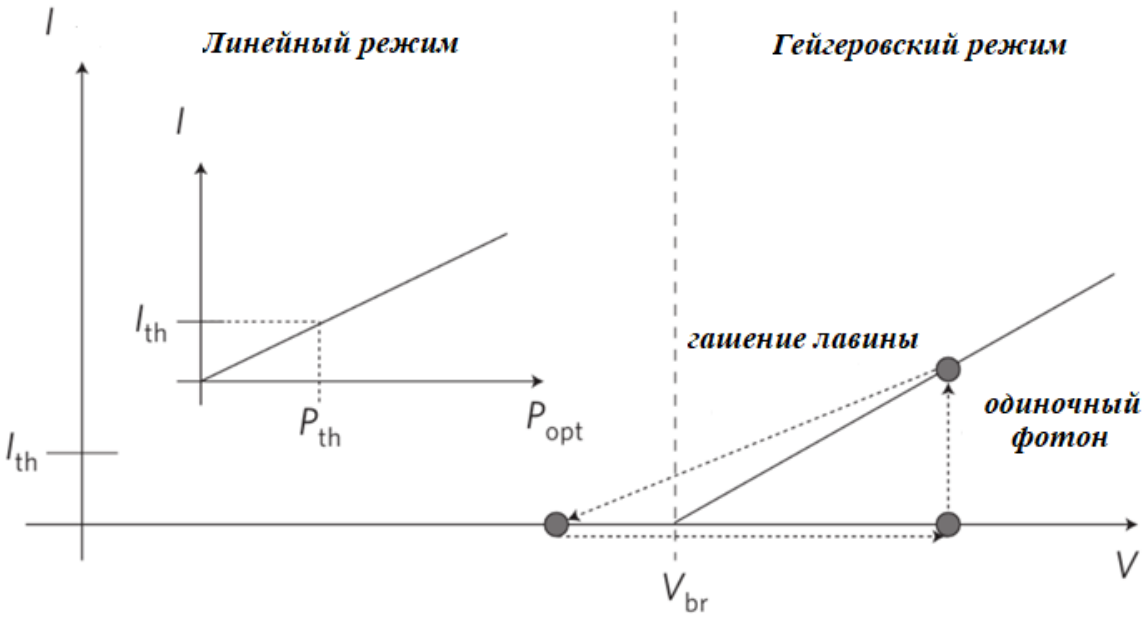


Рисунок 8 – Режимы работы однофотонного ОЛФД

Лавину после пробояОЛФД необходимо остановить (погасить) для последующей работы ОЛФД в режиме счета. Для этого есть несколько способов:

– *пассивный*. Последовательно с детектором ставится резистор большого номинала, при протекании через который тока (еще не приводящего к гибели детектора) происходит падение напряжения, достаточное, что бы напряжение на детекторе упало ниже напряжения пробоя;

– *активный*. При срабатывании детектора на нем сбрасывается напряжение ниже напряжения пробоя и он через некоторое время самовосстанавливается;

– *стробируемый* режим работы. В этом режиме на детектор подается напряжение ниже напряжения пробоя, а в тот момент, когда ожидается регистрация полезного события (появления слабого оптического излучения) подается стробирующий импульс, амплитуда которого вместе со смещением превышает пороговое напряжение пробоя.

В третьем (стробируемом) режиме работает ОЛФД в этой схеме [45].

Для создания строба импульс синхронизации *STR_AMP_IN* поступает через конденсатор на цепочку интегральных усилителей (чтобы из логического сигнала амплитудой 0.8В сделать сигнал амплитудой 6÷7 В), формируя сигнал *APD_STR*.

Для формирования строба на катодОЛФД подается напряжения смещения (постоянное) *APD_BIAS* через балластный резистор (рисунок 6).

АнодОЛФД подключен через резистор на землю. На катод подается положительное напряжения смещения *APD_BIAS* ниже уровня пробоя (около +65В). Через конденсатор подается импульс *APD_STR* (амплитудой 6÷7 В) длительностью ~1.5 нс на половине амплитуды.

При отсутствии напряжения на выходе усилителя конденсатор заряжается до напряжения 65В (выход усилителя – земля). При появлении строба на выходе усилителя формируется напряжение +7В, соответственно на конденсаторе общее напряжение повышается до 72 В относительно земли. Временная диаграмма стробирующих импульсов приведена на рисунке 9, гдеV_{bias} – базовое напряжение, V_{br} – напряжение пробоя ОЛФД.

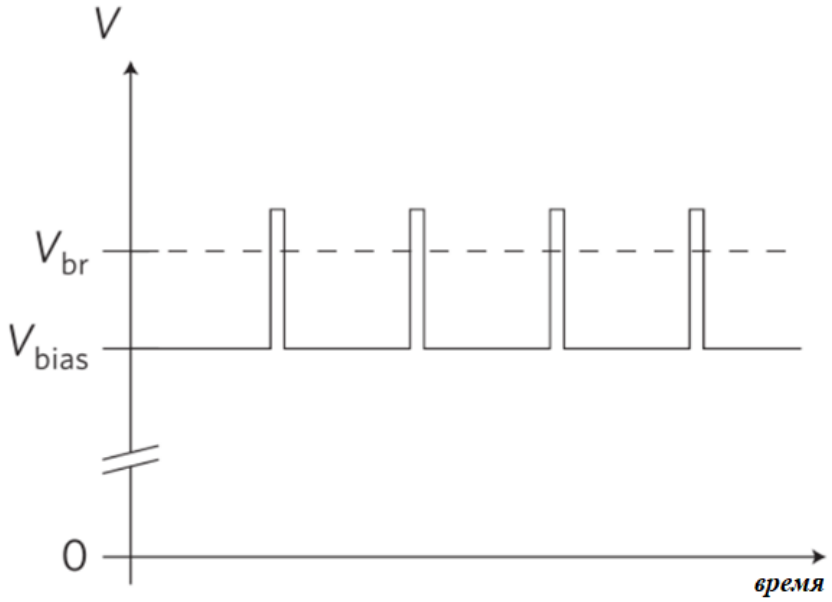


Рисунок 9 – Создание стробирующих импульсов

Обобщая все вышеописанное, получаем следующую структурную схемуи временную диаграмму работы подсистемы синхронизации ДОФ, приведенные на рисунках 10 и 11.

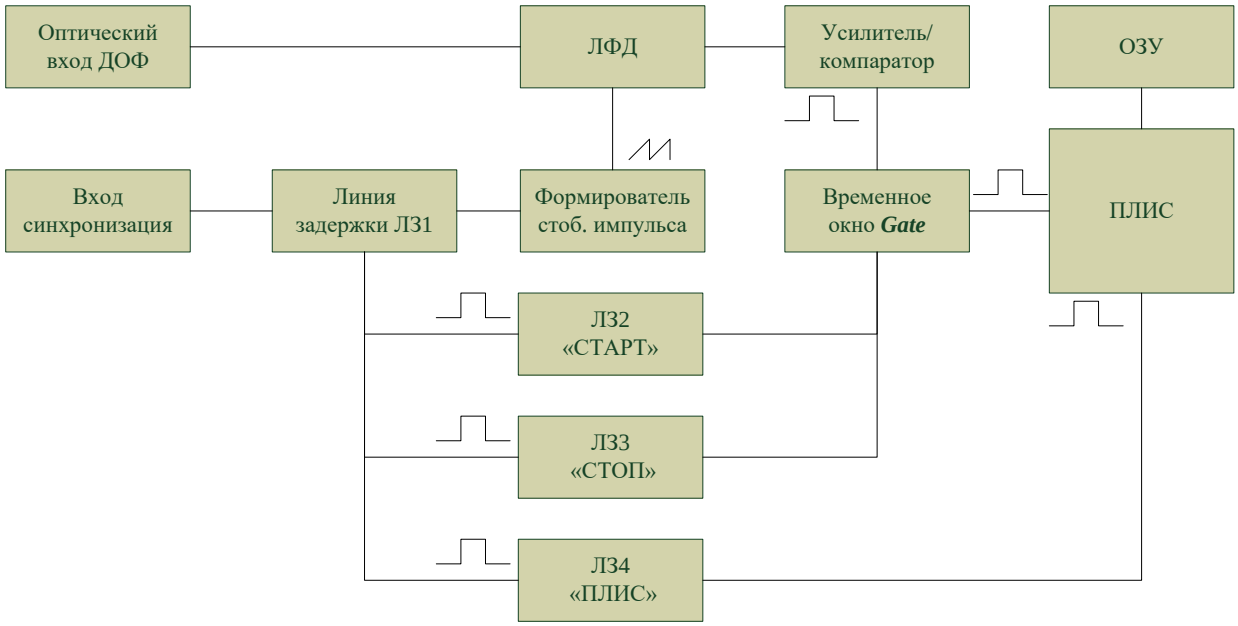


Рисунок 10 – Структурна схема подсистемы синхронизации ДОФ

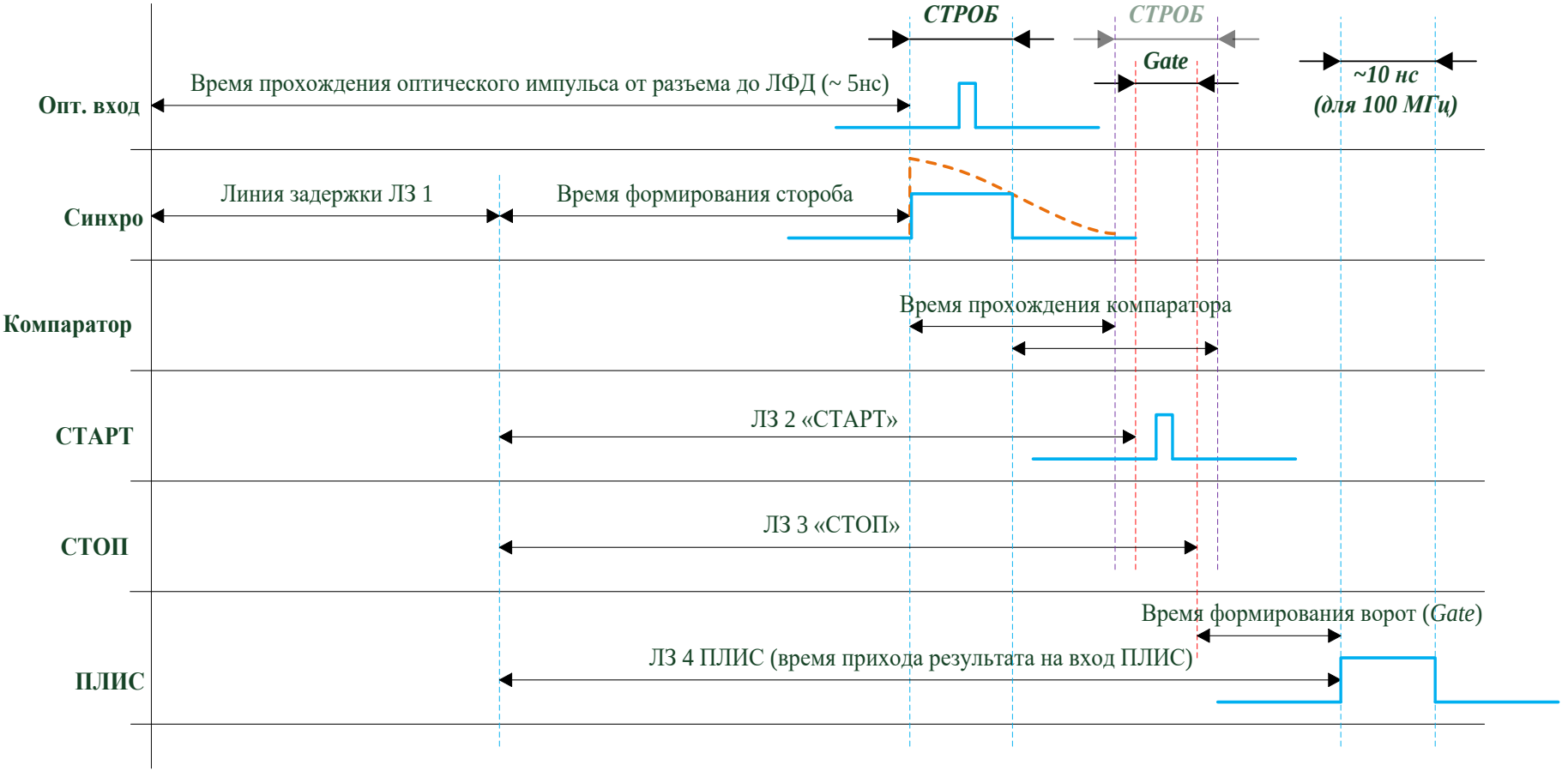


Рисунок 11 – Временная диаграмма работы подсистемы синхронизации ДОФ

1.7 Адаптация ДОФ к работе в общих оптических сетях

ДОФ на основе ОЛДФ нашли широкое применение в квантовой криптографии, при создании разнообразных систем квантового распределения ключей. Данные изделия получаются компактными, быстродействующими с относительно низким энергопотреблением.

Однако реализация возможности работы аппаратуры КРК в общих оптических сетях при объединении квантовых и классических сигналов накладывает определенные требования к ДОФ, большинство из которых обусловлено наличием шумовых квантовых состояний при работе аппаратуры КРК.

С одной стороны, для унификации ДОФ как некоего абстрактного устройства, необходимо уметь регулировать квантовую чувствительность, ширину строба и «мертвое» время (время восстановления после срабатывания).

С другой стороны, для противодействия шумовым квантовым состояниям в ДОФ должна быть реализована защита от перевода ОЛФД в линейный режим и ложных срабатываний.

Предложенное в [45] техническое решение позволяет создать ДОФ на основе однофотонного лавинного фотодиода (ОЛФД) с достаточно хорошими характеристиками. Однако данное техническое решение имеет ряд недостатков:

– фиксированная физическая длительность стробирующего импульса (строба), не коррелирующая с длительностью временных ворот;

– отсутствие схемы активного гашения лавины для снижения «мертвого времени» ДОФ (запрет на стробы во время восстановления ОЛФД после лавины);

– отсутствие контроля перевода ОЛФД в линейным режим посредством внешнего оптического излучения.

1.7.1 Фиксированная физическая длительность строба.Для формирования электрического стробирующего импульса в [45] используется схема на конденсаторе (рисунок 6). Емкость конденсатора подбирается таким образом, чтобы обеспечить необходимую длительность строба относительно

длительности временных ворот. Однако при разрядке конденсатора через ОЛФД (темновой ток) напряжение на нём уменьшаетсяпо ниспадающей (рисунок 12).

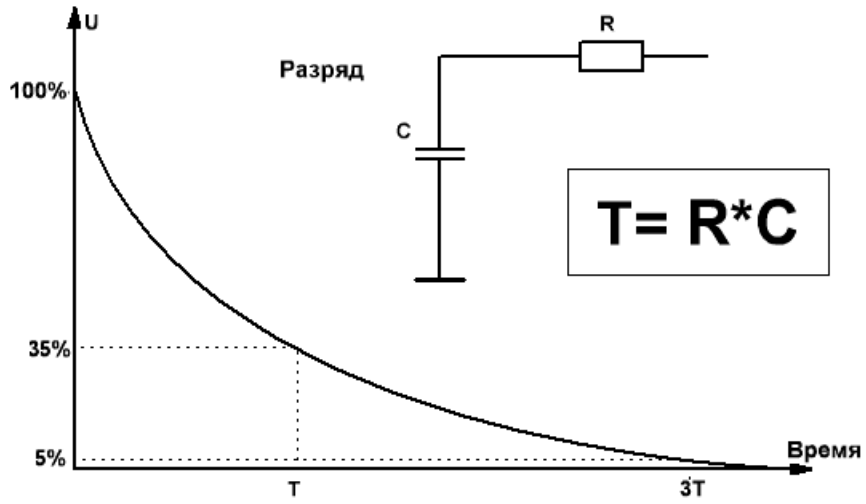


Рисунок 12 – Временная диаграмма разрядки конденсатора

Применение конденсатора в схеме формирования стробов приводит к тому, что в начале строба напряжение больше, чем в конце строба, причем за пределами строба наблюдается остаточное напряжение на конденсаторе, которое может приводить к ложному срабатыванию ДОФ. Также необходимо отметить, что квантовая эффективность ОЛФД пропорциональна приложенному обратному напряжению, превышающему напряжение пробоя. Следовательно, ДОФ будет иметь квантовая эффективность в начале строба больше, чем в конце строба.

Таким образом, применение конденсатора с большей емкостью сгладит разность квантовой эффективности ДОФ в начале и конце импульса, но увеличит вероятность ошибочного (темнового) срабатывания ОЛФД уже за пределами временных ворот. А применение конденсатора с меньшей емкостью снизит общую квантовую эффективность ДОФ.

Для решения этой задачи была предложена электрическая схема формирования строба на TTL-логике, приведенная на рисунке 13[47].

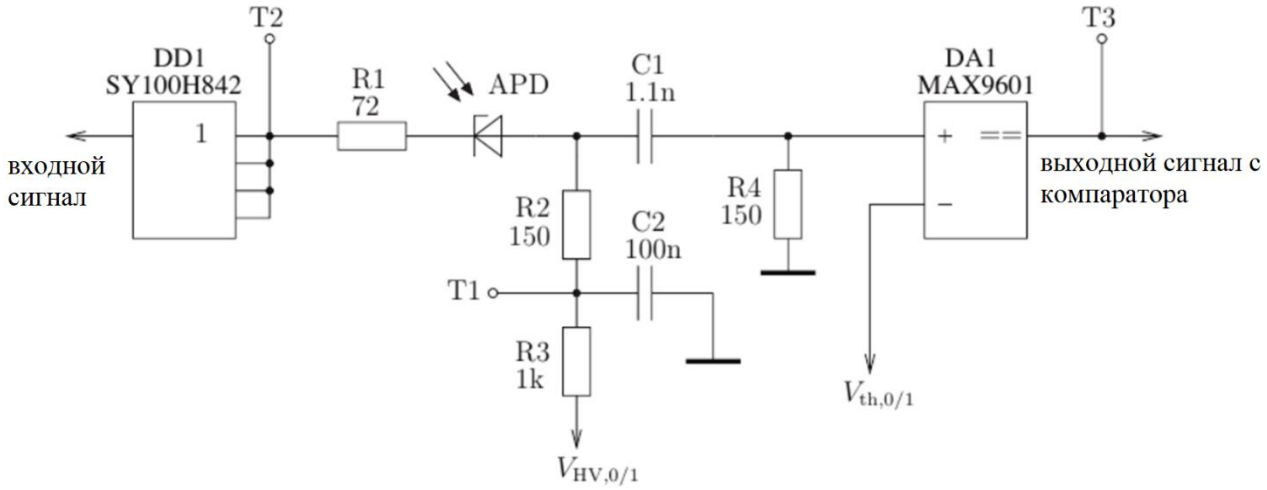


Рисунок 13 – Электрическая схема формирования строба

Данная схема управления и формирования строба позволяет как сделать прямоугольный строб, выравнивая квантовую эффективность ОЛФД в течении строба, так и физически менять его длительность относительно длительности временных ворот.

1.7.2 Система активного гашения лавины ОЛФД.После срабатывания ОЛФД ему требуется некоторое время на восстановление – завершения процесса рассасывания носителей лавины. Иначе, подача очередного строба на ОЛФД в промежуток времени, пока в объемной структуре ОЛФД сохраняются заряженные эпицентры, вызовет повторное срабатывание ОЛФД даже при отсутствии оптического излучения на входе. В таких условия процесс появление повторных лавин будет бесконечным.

Данный временной промежуток, в течении которого происходит восстановление ОЛФД, называют «мертвым» временем. То есть в течении мертвого времени блокируется подача стробирующих импульсов на ОЛФД. Временная диаграмма работы ОЛФД с активным гашением лавины приведена на рисунке 14.

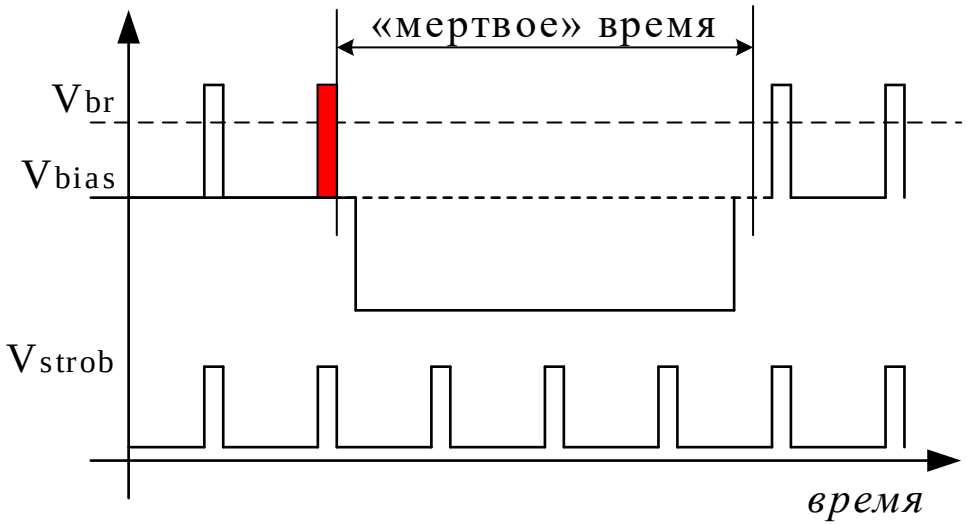


Рисунок 14 – Временная диаграмма мертвого времени ОЛФД

Базовым механизмом гашения лавины, когда ОЛФД работает в стробируемом режиме, и восстановление ОЛФД происходит пассивно при подаче обратного напряжения, не превышающего напряжение пробоя, является блокировка выработки стробирующих импульсов [45].

Наряду с базовым режимом можно использовать активный режим гашения лавины. Для этого во временном интервале мертвого времени отключается источник высокого напряжения (или снижается на нем напряжения [49]). Данный механизм позволяет ускорить процесс рассасывание носителей лавины, уменьшая необходимое время на восстановление ОЛФД с сотен до единиц микросекунд. Частично данный механизм реализован на схеме, приведенной на рисунке 15, когда сигнал с выхода схемы регистрации срабатывания ОЛФД используется для снижения напряжения постоянного высоковольтного источника питания ОЛФД.

Также существуют специализированные микросхемы для высоковольтного питания ОЛФД, в которых уже реализован механизм снижения напряжения после срабатывания ОЛФД.

1.7.3 Защита от перевода ОЛФД в линейный режим

Защита от перевода ОЛФД в линейный режим – защита от ослепления – строится на основе контроля тока через ОЛФД [49].

Электрическая схема контроля тока через ОЛФД приведена на рисунке 15. Данная схема полностью совместима со схемой прямоугольных стробирующих импульсов (рисунок 13), позволяя реализовать требуемые характеристики и механизмы в одном изделии.

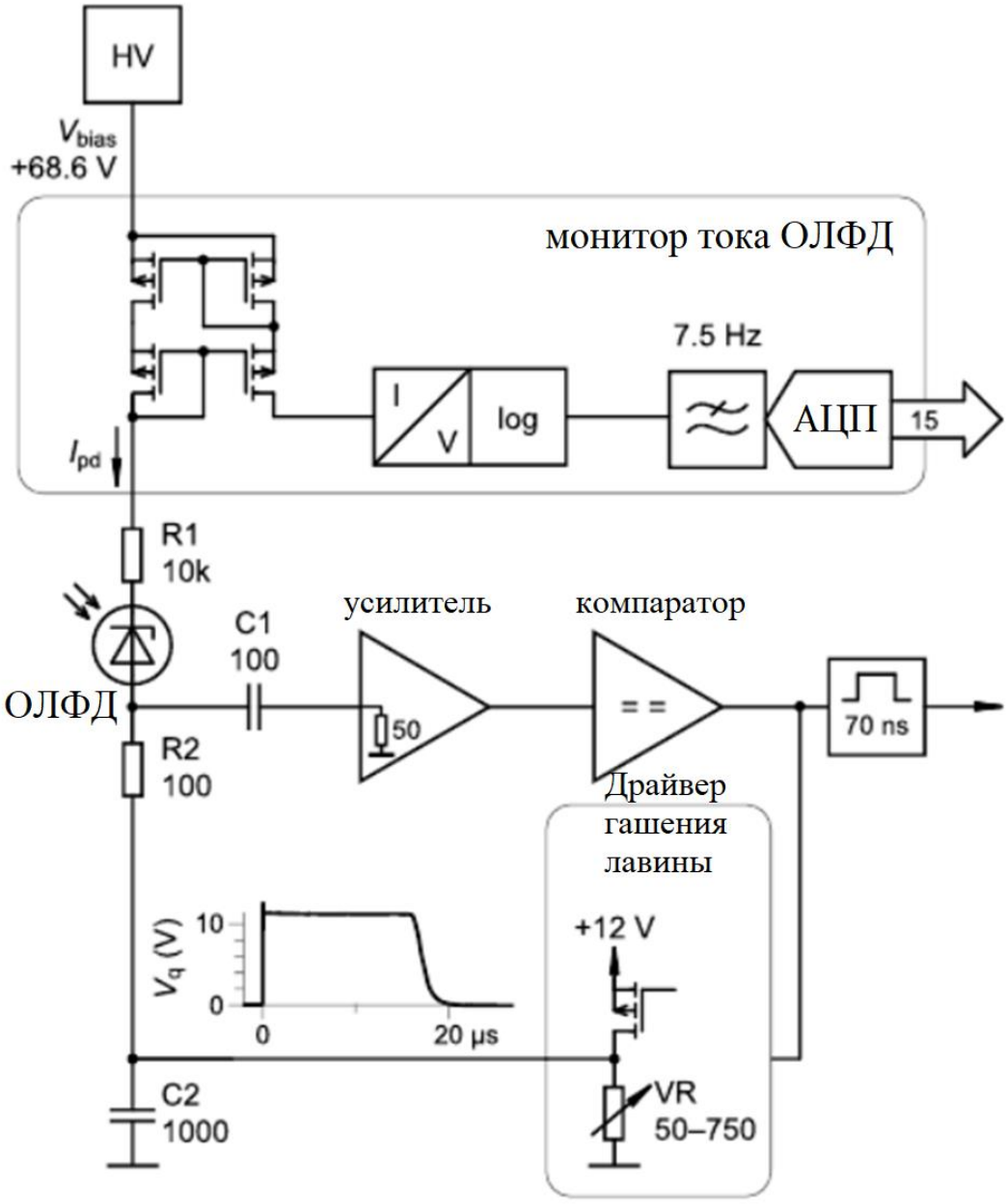


Рисунок 15 – Электрическая схема контроля тока через ОЛФД

Для контроля тока через ОЛФД используется схема зеркалирования тока на полевых транзисторах с преобразователем тока в напряжение и аналогово-цифровым преобразователем.

2 Экспериментальная работа по моделированиюсовместной передачи классических и квантовых сигналов в одном волокне

2.1 Структурная схема адаптированного ДОФ

ДОФ предназначен для регистрации сильно-ослабленных оптических импульсов в заданные временные интервалы по внешнему сигналу синхронизации.

Структурная схема ДОФ приведена на рисунке 16.

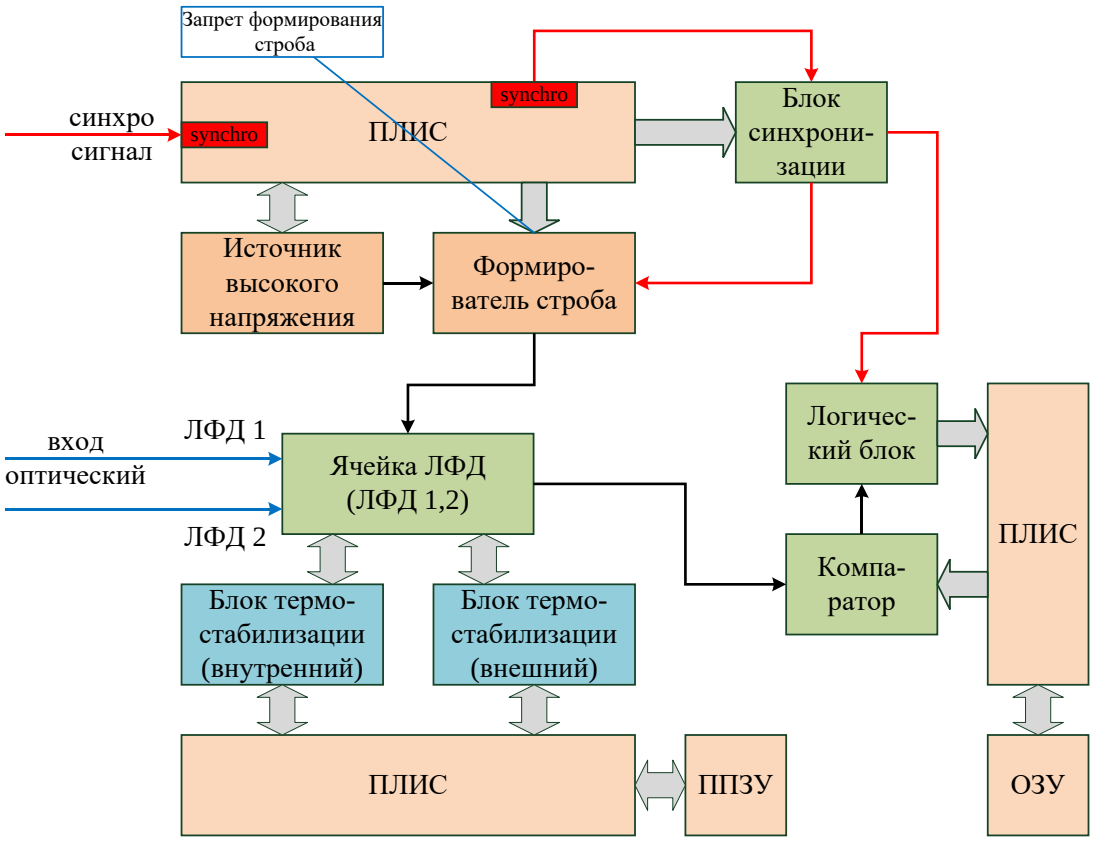


Рисунок 16 – Структурная схема ДОФ

Основными структурными блоками ДОФ являются:

– блок синхронизации функциональных блоков ДОФ;

– блок ПЛИС с АРМ-процессором ипамятью (ОЗУ и ППЗУ);

– блок термостабилизации ОЛФД (внешний и внутренний);

– блок источник питания ОЛФД высокого напряжения;

– блок формирования стробирующего импульса;

– блок компаратора ОЛФД (регистрация срабатывания ОЛФД в заданном временном окне);

– блок логической обработки сигналов ОЛФД.

Особенностью применяемого ОЛФД является размещение в одном корпусе как оптически-чувствительного элемента, так и внутреннего охладителя (элемента Пельтье). Поэтому ОЛФД входит в состав как блока компаратора ОЛФД, так и в блок термостабилизации ОЛФД.

2.1.1 Блок ПЛИС с процессором и модулем памяти. Используется готовая коммерческая электрическая плата с ПЛИС, содержащей в себе *ARM*-процессор, и ОЗУ.

2.1.2 Блок синхронизации функциональных блоков ДОФ состоит из двух схем:

– схема формирования синхроимпульса;

– схема распределения синхроимпульса (синхронизация работы структурных блоков ДОФ).

Схема формирования синхроимпульса приведена на рисунке 17.

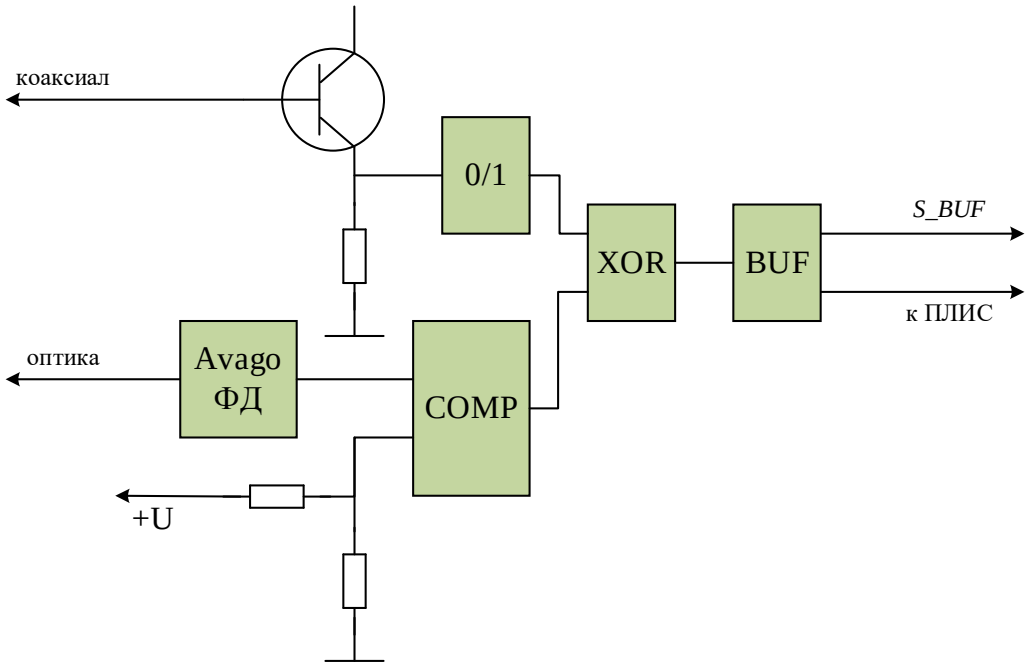


Рисунок 17 – Схема формирования синхроимпульса

Схема формирования синхроимпульса имеет два входа – оптический и электрический. Использование конкретного входа определяется внешней коммутацией ДОФ.

Сформированный импульс синхронизации *S_BUF* подается в ПЛИС и на схему распределения синхроимпульса.

Схема распределения синхроимпульса между структурными блоками ДОФ приведена на рисунке 18.

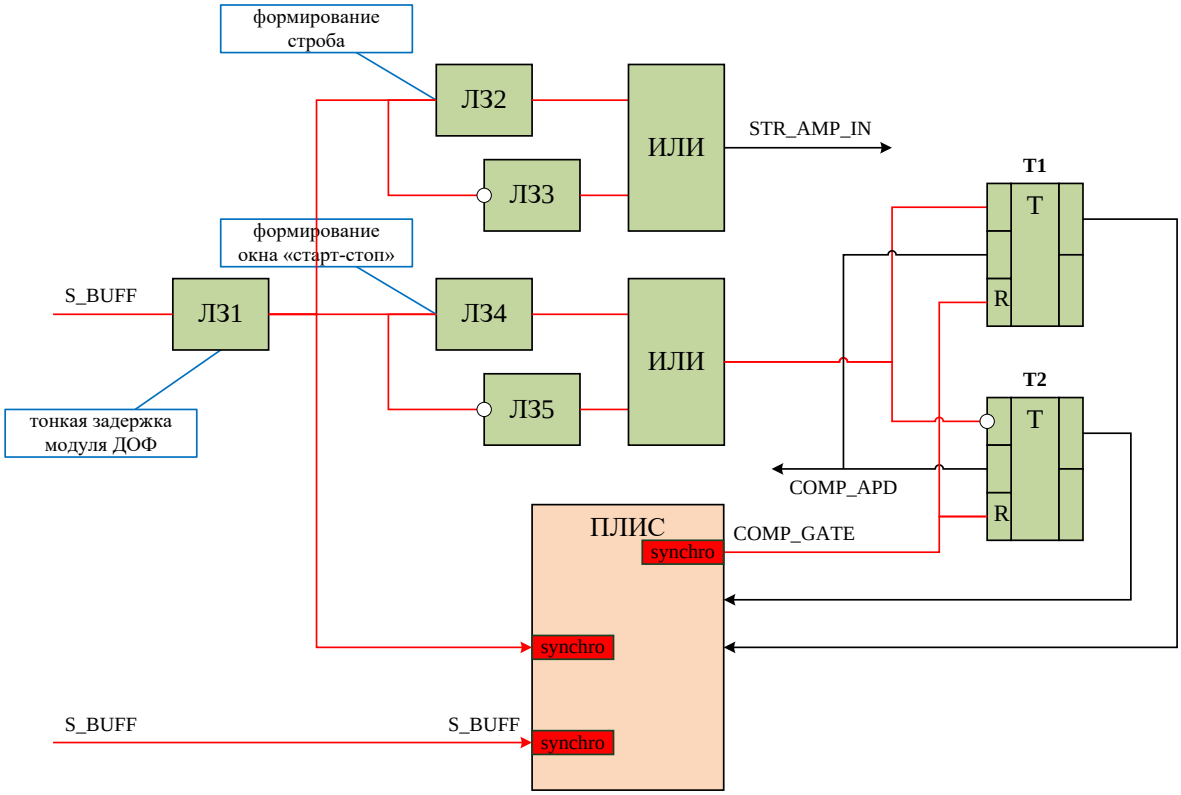


Рисунок 18 – Схема распределения синхроимпульса по блокам ДОФ

Значения временных задержек линий задержек ЛЗ1, ЛЗ2, …, ЛЗ5 устанавливаются процессором ПЛИС.

Импульс синхронизации *S_BUF* подается на вход линии задержки ЛЗ1, которая согласует время прохождения оптического импульса по оптическому волокну ОЛФД и электрических импульсов управления ОЛФД.

Далее импульс синхронизации подается на вход:

– ПЛИС;

– линию формирования строба *STR_AMP*;

– линию формирования временного окна «старт-стоп» (*GATE*).

Сигнал формирования строба *STR_AMP_IN1* используется в блоке формирования стробирующего импульса.

Сигнал формирования гейта управляет триггерами *T1* и *T2*, которые обрабатывают сигналы от компаратора ОЛФД (сигнал *COMP_APD*).

2.1.3 Блок термостабилизации ОЛФД используется для установки рабочей температуры ОЛФД.

Рекомендованная рабочая температура:

– кристалла ОЛФД равна «–40»°С;

– корпуса ОЛФД равна 20°С.

В конструкции ДОФ используется два блока термостабилизации:

– внутренний, для установки рабочей температуры кристалла ОЛФД (терморезистор и элемент Пельтье размещены внутри корпуса ОЛФД);

– внешний, для установки рабочей температуры корпуса ОЛФД (терморезистор и элемент Пельтье внешние, относительно корпуса ОЛФД).

Схемы управления внешним и внутренним блоком термостабилизации одинаковые. Схема управления приведена на рисунке 19.

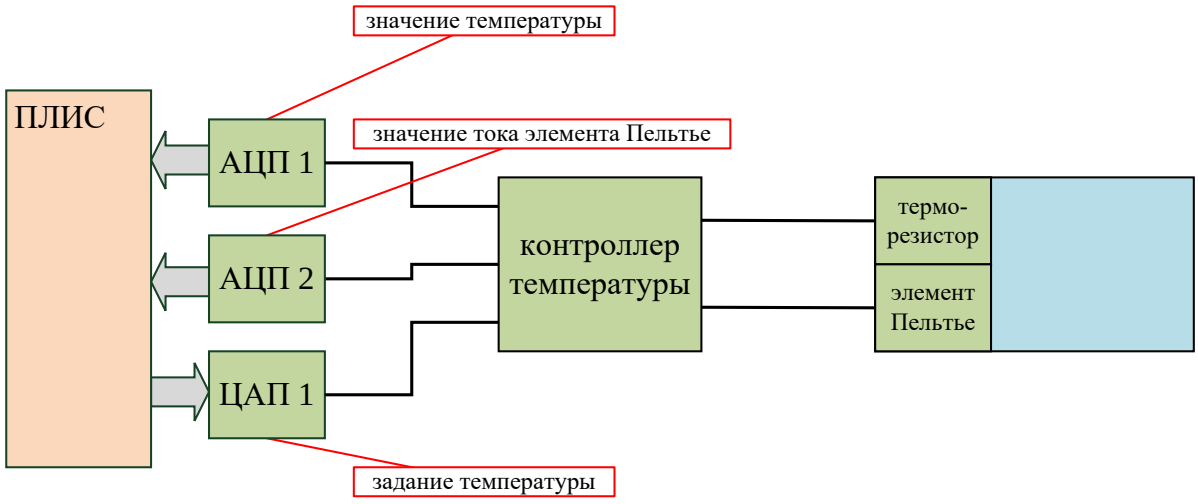


Рисунок 19 – Схема блока термостабилизации

Для каждого ЦАП/АЦП в процессоре ПЛИС используются калибровочные таблицы, которые ставят в соответствие управляющим кодам ЦАП/АЦП значения физических величин (температуры или тока).

Для работы блока термостабилизации ОЛФД используется 6 калибровочных таблиц (3 для внутреннего и 3 для внешнего блока термостабилизации).

При первом запуске ДОФ используются типовые калибровочные таблицы, рассчитанные под заявленные характеристики элементов (терморезисторы, резисторы в схеме питания элемента Пельтье, аналоговый вход микросхемы контроллера температуры).

В процессе калибровки ДОФ значения таблиц уточняются под конкретные элементы по результатам измерения физических величин.

2.1.4 Для формирования стобирующего импульса ОЛФД используется регулируемый источник высокого напряжения.

Структурная схема источника высокого напряжения приведена на рисунке 20.

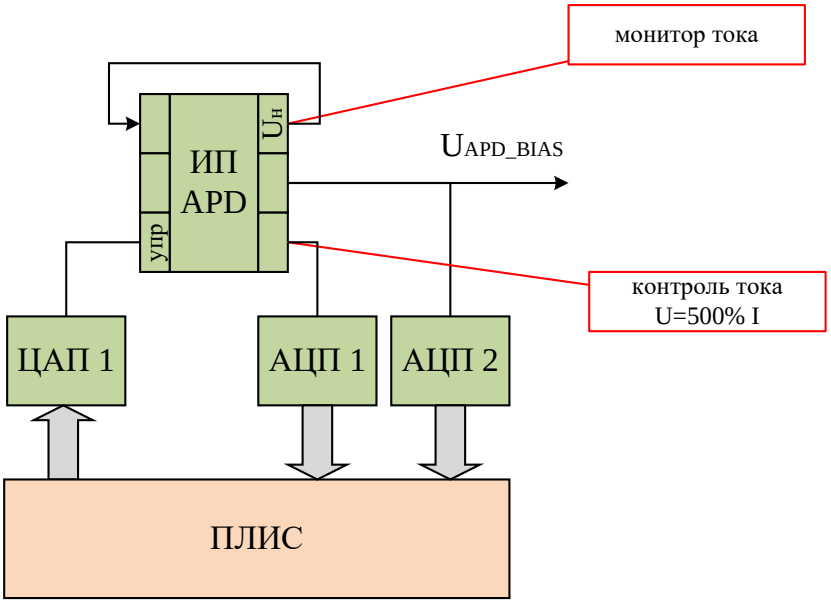


Рисунок 20 – Схема источника высокого напряжения

Для формирования высокого напряжения используется специализированная микросхема, управление которой выполняется аналоговыми линиями. Для согласования аналоговых линий с цифровыми линиями ПЛИС используются ЦАП и АЦП:

– ЦАП1 задает необходимое напряжение на выходе микросхемы;

– АЦП2 контролирует напряжение на выходе микросхемы;

– АЦП1 контролирует ток на высоковольтном выходе микросхемы.

Для работы блока источника высокого напряжения используются калибровочные таблицы для ЦАП/АЦП, описывающие соотношение управляющих кодов и физических величин (напряжение и ток).

При первом запуске ДОФ используются типовые калибровочные таблицы, далее в процессе калибровки ДОФ значения таблиц уточняются под конкретные элементы по результатам измерения физических величин.

2.1.5 Блок компаратораОЛФД.Для регистрации срабатывания ОЛФД используется компаратор, который обеспечивает фильтрацию полезного сигнала от случайных шумов.

Структурная схема блока компаратора приведена на рисунке 21.

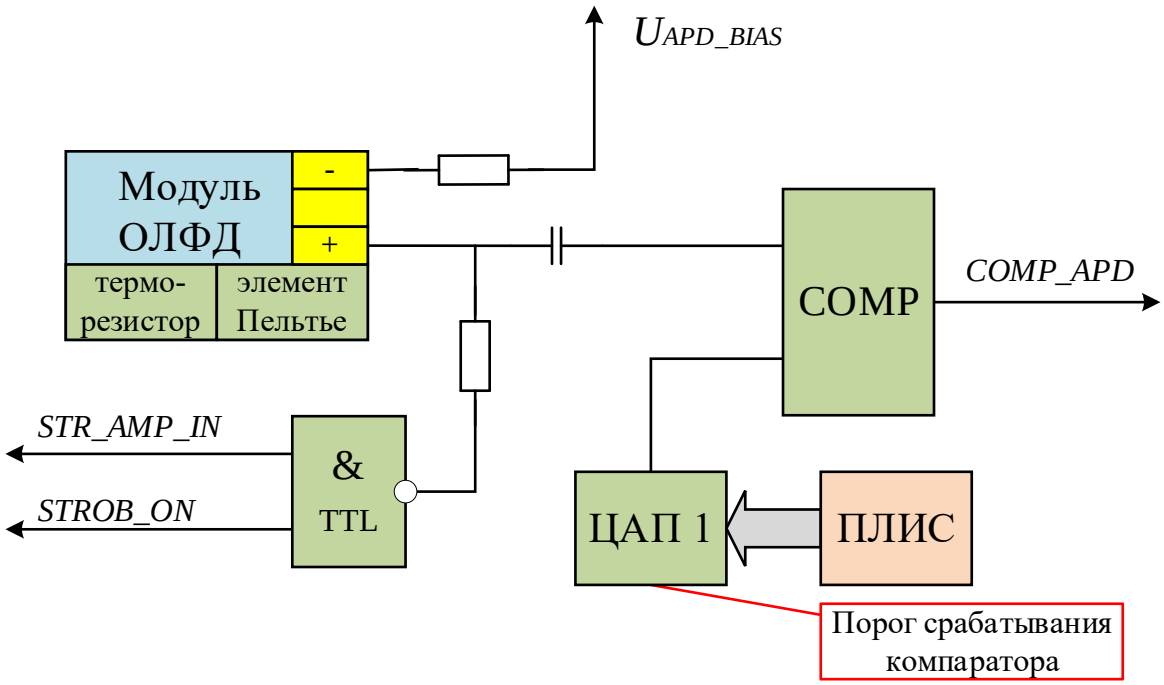


Рисунок 21 – Схема компаратора ОЛФД

Первый вход компаратора подключен к катоду ОЛФД через конденсатор. При срабатывании ОЛФД происходит его пробой, что вызывает резкое увеличение тока в цепи его питания. Увеличение тока приводит к увеличению напряжения на резисторе, подключенному к катоду (+) ОЛФД, и соответственно заряду конденсатора, формируя импульс на первом входе компаратора. Конденсатор ограничивает длительность информационного импульса о срабатывании ОЛФД.

На второй вход компаратора подается постоянное напряжение с выхода ЦАП1, управляемого ПЛИС. Данный вход компаратора задает порог срабатывания компаратора.

При превышении напряжения на первом входе по отношению ко второму входу компаратор формирует импульс *COMP_APD*, который далее подается в логический блок обработки сигналов ОЛФД (см. рисунок 18).

Для работы блока компаратора используется калибровочная таблица для ЦАП, определяющая соотношение управляющих кодов и физической величины (напряжение, мВ).

2.1.6 Блок формирования стробирующих импульсов ОЛФД.Для превышения обратного напряжения на ОЛФД выше напряжения пробоя в заданные временные интервалы используются стробирующие импульсы.

Для формирования стробирующего импульса используется логический элемент «ИЛИ» быстродействующей *TTL* логики, к инверсному выходу которого подключен катод ОЛФД (рисунок 21). В обычном состоянии на инверсном выходе присутствует сигнал логической единицы, соответствующий напряжению питания микросхемы. Для формирования стробирующего импульса элемент переводится в логический ноль, замыкая резистор катода на землю. В результате напряжение на ОЛФД увеличивается на разность напряжений, соответствующим логическому уровню нуля и единицы. Для формирования стробирующего импульса достаточно прироста напряжения на ОЛФД на 5-6 вольт.

На входы элемента «ИЛИ» подаются сигналы *STR_AMP_IN* и *STROB_ON*. Сигнал *STR_AMP_IN* определяет момент начала стробирующего импульса и его длительность. Сигнал *STROB_ON* задается ПЛИС и разрешает формирование стробирующего импульса.

После срабатывания ОЛФД (возникновения пробоя) требуется некоторое время до 50 мкс на восстановление электронной структуры зарядов в объеме кристалла ОЛФД. Появление стробирующего импульса в данный временной интервал приведёт к повторному срабатыванию ОЛФД. Поэтому после

срабатывания ОЛФД вводится запрет на формирование стробирующих импульсов на время релаксации ОЛФД. Значение времени релаксации подбирается индивидуально для каждой модели ОЛФД и хранится в ППЗУ ДОФ.

2.2 Параметрыконфигурации ДОФ

Основные параметры конфигурации ДОФ разделены на две группы:

– параметры, доступные для настройки пользователем;

– параметры, недоступные пользователю.

Для настройки параметров конфигурации ДОФ пользователь должен использовать системное программное обеспечение, предоставляемое разработчиком ДОФ.

Разработчик ДОФ для калибровки и конфигурирования ДОФ должен использовать специализированное программное обеспечение, недоступное обычному пользователю.

Все параметры конфигурации ДОФ хранятся в ППЗУ ДОФ.

2.2.1 Параметры, доступные для настройки пользователем.Пользователю при работе с ДОФ доступны следующие параметры:

– время малой задержки ДОФ (значение линии задержки ЛЗ1, рисунок 18), значение задается в интервале 0 – 10 нс, с шагом 0,05 нс;

– ширина гейта (временных ворот «Старт-Стоп»), значение задается в интервале 0,1 – 5 нс, с шагом 0,05 нс (значение линий задержек ЛЗ2,3 и ЛЗ4,5 рассчитываются автоматически);

– квантовая эффективность (определяется амплитудой стробирующего импульса), значение задается в интервале 5 – 25%, с шагом в 1%;

– время релаксации ОЛФД («мертвое» время), значение задается в интервале 0,1 – 50 мкс, с шагом 0,1 мкс (примечание – минимальное значение определяется при калибровке ДОФ).

2.2.2 Параметры, задаваемые при калибровке ДОФ.Во время калибровки ДОФ задаются следующие параметры (недоступны пользователю без специального ПО):

– температура кристалла ОЛФД, значения задаются в интервале 0 – «-60»°С с шагом 1°С, рекомендуемое значение равно «–40»°С (примечание – внутренний элемент Пельтье может создать разницу температур «корпус-кристалл» до 60°С);

– температура корпуса ОЛФД, значения задаются в интервале 0 – 30°С с шагом 1°С, рекомендуемое значение равно +20°С (примечание – при температуре корпуса ОЛФД ниже +10°С может произойти образование конденсата, что должно быть учитывать при разработке корпуса ДОФ);

– скорость охлаждения ОЛФД (корпус и кристалл), рекомендуемое значение 1°С/сек. (более быстрое охлаждение может привести к механическим повреждениям ОЛФД);

– рабочее напряжение ОЛФД, значения задаются в интервале 40 – 80 В, с шагом 0,05 В (примечание – при заводской настройке создается калибровочная таблица между рабочим напряжением ОЛФД и квантовой эффективностью ДОФ);

– значение напряжения компаратора ОЛФД, значения задается в интервале 0 – 2 В с шагом 0,01 В, рекомендуемое значение определяется при калибровке ДОФ, как оптимальное соотношение между чувствительностью и уровнем шумов;

– калибровочные таблицы температур, напряжений и токов;

– частота темнового счета (определяется по результатам калибровки ДОФ, дается несколько значений при разной квантовой эффективности и длительности стробирующего импульса).

2.3 Алгоритм работы ДОФ.

ДОФ может находиться в нескольких режимах работы:

– режим инициализации;

– режим ожидания;

– режим работы (рабочий режим).

В режим инициализации ДОФ автоматически переходит сразу после подачи на него питания. После достижения заданных параметров работы ДОФ автоматически переходит в режим ожидания.

Для перевода ДОФ в рабочий режим работы системное программное обеспечение (СПО) пользователя отправляет в ДОФ команду «СТАРТ», после чего ДОФ готов регистрировать входящее оптическое излучение. В ответ на команду «СТАРТ» ДОФ сообщает значение максимального количества измерений, которое может сохранить в своей памяти.

В параметрах команды «СТАРТ» указывается ожидаемое количество синхроимпульсов (количество измерений), либо указывается производить измерения до заполнения оперативной памяти ДОФ.

По окончании измерений (отработаны заявленное количество синхроимпульсов или закончилась ОЗУ) ДОФ автоматически переходит в режим ожидания. Если необходимо прервать процесс измерений, то ДОФ необходимо принудительно перевести в режим ожидания командой «СТОП» с помощью СПО пользователя.

В режиме ожидания из ДОФ можно считать результаты измерений единым блоком.

СПО пользователя имеет функционал считывания из ОЗУ ДОФ результаты измерения в режиме реального времени.

2.3.1 Инициализация ДОФ. После подачи питания на ДОФ процессор ПЛИС выполняет следующие действия:

1) считывает из ППЗУ базовые настройки (рабочая температура корпуса и кристалла ОЛФД, рабочее напряжение ОЛФД, пороговое напряжение компаратора ОЛФД, временные задержки блока синхронизации, калибровочные таблицы), примечание – калибровочные таблицы используются процессором для преобразования физических величин (ток, напряжение, температура) в бинарные коды при управлении и/или чтении ЦАП/АЦП;

2) блокирует источник высокого напряжения ОЛФД;

3) устанавливает запрет на выработку стробирующих импульсов;

4) запускает процесс установки рабочей температуры ОЛФД;

5) устанавливает временные задержки блока синхронизации;

6) устанавливает пороговое напряжение компаратора ОЛФД;

7) устанавливает рабочее напряжение источника высокого напряжения;

После выхода на заданные параметры работы (температура ОЛФД, установка значений ЦАП/АЦП и значений линий задержек блока синхронизации) работа ДОФ в режиме инициализации считается законченной.

После инициализации ДОФ переходит в режим ожидания.

2.3.2 Режим ожидания ДОФ.В режиме ожидания ДОФ выполняет следующие функции:

– поддерживает рабочую температуры ОЛФД и работу блока источника высокого напряжения;

– сохраняет запрет на выработку стобирующих импульсов;

– игнорирует импульсы синхронизации и оптические импульсы, приходящие на ОЛФД.

2.3.3 Рабочий режим ДОФ. После получения команды «СТАРТ» на переход в рабочий режим процессор ПЛИС:

1) очищает область ОЗУ, предназначенную для хранения номеров срабатываний ОЛФД относительно синхроимпульсов;

2) разрешает формирование стробирующих импульсов по импульсам синхронизации;

3) после подготовки ДОФ отправляет ответ об успешном переходе в рабочий режим.

2.4 Обработка и передача результатов измерения

В ходе своей работы ДОФ накапливает результаты измерений и периодически их передает в сопряженные модули.

2.4.1 Хранение результатов измерения в памяти. Хранение номеров отсчетов в ОЗУ выполняется следующим образом.

Работа ДОФ в рабочем режиме подчиняется импульсам синхронизации. В ПЛИС организован счётчик синхроимпульсов. Каждому значению счетчика соответствует определенный бит в ОЗУ (по смещению, определяемому значение счетчика импульсов синхронизации).

Если во временной интервал *GATE* (ворота «старт-стоп»), соответствующий текущему импульсу синхронизации было зафиксировано срабатывание ОЛФД, в ОЗУ по текущему смещению записывается бит «1», иначе бит «0».

Примечание. На время релаксации ОЛФД по синхроимпульсам в ОЗУ записываются биты «0».

2.4.2 Получение результатов измерений – вычитывание результатов измерения происходит в режиме ожидания.

После получения импульсов синхронизации в количестве, указанном в команде «СТАРТ» перехода рабочий режим, ДОФ автоматически переходит в режим ожидания. Чтобы не испортить результаты измерения запрещается увеличение счетчика импульсов синхронизации и формирование новых стробирующих импульсов.

2.4.3 Динамический режим считывания результатов. Одной из вариаций рабочего режима работы ДОФ является подрежим динамического считывания результатов измерений. В подрежиме динамического считывания хранениерезультатов измерений обеспечивается СПО пользователя, снимая ограничения на физическую память ДОФ.

Для подрежима динамического считывания ОЗУ ДОФ разделяется на блоки небольшого размера, из которых образуется кольцевой буфер записи. Вычитывания блоков записи происходит в рабочем режиме работы ДОФ. После вычитывания заполненного блока ОЗУ с результатами измерений, данный блок помечается свободным и готовым к записи результатов измерений. За формирование и отслеживание последовательности заполнения блоков памяти

в процессе работы ДОФ, а также их освобождение после вычитывания, отвечает процессор ПЛИС.

Для останова процесса измерений СПО пользователя должно отправить команду «СТОП», что переведет ДОФ в режим ожидания.

Примечание – несвоевременное вычитывание блоков памяти СПО пользователя может привести к переполнению памяти ДОФ. В данном случае автоматического останова работы ДОФ с переводом в режим ожидания не произойдет, а данные начнут записываться в блок памяти с самыми старыми результатами измерений.

3 Расчет экономической эффективности

Результатом научно-исследовательской работы (НИР) является достижение научного, научно-технического, экономического и социального эффектов.

1. Научный эффект характеризуется получением новых научных знаний и отражает прирост информации, предназначенной для «внутри научного» потребления.

2. Научно-технический эффект характеризует возможность использования результатов выполняемых исследований в других НИР и обеспечивает получение информации, необходимой для создания новой продукции.

3. Экономический эффект характеризует коммерческий эффект, полученный при использовании результатов прикладных НИР.

4. Социальный эффект проявляется в улучшении условий труда, повышении экономических характеристик, развитии культуры, здравоохранения, науки, образования.

Научная деятельность носит многоаспектный характер, ее результаты, как правило, могут использоваться во многих сферах экономики в течение длительного времени.

Оценка научной и научно-технической результативности НИР производится с помощью системы взвешенных балльных оценок. Для фундаментальных НИР рассчитывается только коэффициент научной результативности (таблица 4), а для поисковых работ и коэффициент научно-технической результативности (таблица 5). Оценки коэффициентов могут быть установлены только на основе опыта и знаний научных работников, которые используются как эксперты, путем сопоставления достигнутых параметров с базовыми.

Таблица 4 – Характеристики факторов и признаков научной результативности

Фактор научной результатив-ности	Коэф. значимости фактора	Качество фактора	Характеристика фактора	Коэф. достигнутого уровня
Новизна полученных результатов	0,5	Высокая	Принципиально новые результаты, новая теория, открытие новой закономерности	1,0
		Средняя	Некоторые общие закономерности, методы, способы, позволяющие создать принципиально новую продукцию	0,7
		Недоста-точная	Положительное решение на основе простых обобщений, анализа связей факторов, распространение известных принципов на новые объекты	0,3
		Тривиаль-ная	Описание отдельных факторов, распространение ранее полученных результатов, реферативные обзоры	0,1
Глубина научной проработки	0,35	Высокая	Выполнение сложных теоретических расчетов, проверка на большом объеме экспериментальных данных	1,0
		Средняя	Невысокая сложность расчетов, проверка на небольшом объеме экспериментальных данных	0,6
		Недоста-точная	Теоретические расчеты просты, эксперимент не проводился	0,1
Степень вероятности успеха	0,15	Большая		1,0
		Умеренная		0,6
		Малая		0,1

Таблица 5 – Характеристики факторов и признаков научно-технической результативности

Фактор научно-технической результативности	Коэф. значимости фактора	Качество фактора	Характеристика фактора	Коэф. достигнутого уровня
Перспектив-ность использования результатов	0,5	Перво-степенная	Результаты могут найти применение во многих научных направлениях	1,0
		Важная	Результаты будут использованы при разработке новых технических решений	0,8
		Полезная	Результаты будут использованы при последующих НИР и разработках	0,5
Масштаб реализации результатов	0,3	Национальная экономика	Время реализации: до 3 лет, до 5 лет, до 10 лет, свыше 10 лет	 1,0 0,8 0,6 0,4
		Отрасль	Время реализации: до 3 лет, до 5 лет, до 10 лет, свыше 10 лет	 0,8 0,7 0,5 0,3
		Отдельные фирмы и предприя-тия	Время реализации: до 3 лет, до 5 лет, до 10 лет, свыше 10 лет	 0,4 0,3 0,2 0,1
Завершенность результатов	0,2	Высокая	Техническое задание на ОКР	1
		Средняя	Рекомендации, развернутый анализ.	0,6
		Недоста-точная	Обзор, информация	0,4

Коэффициента научной результативности ($k_{\text{н.р.}}$) определяется по формуле:

$$k_{\text{н.р.}} = \sum_{i=1}^{n} k_{\text{зн.}i} \cdot k_{\text{д.у}\,i} \,, \qquad (3.1)$$

где$k._{\text{зн.i}}$ – коэффициент значимости *i*-го фактора, $k._{\text{зн.i}}$ – коэффициент достигнутого уровня для *i*-го фактора.

Коэффициента научно-технической результативности ($k._{\text{нт.р.}}$) определяется по формуле:

$$k_{\text{нт.р.}} = \sum_{i=1}^{n} k_{\text{зн.}i} \cdot k_{\text{д.у}\,i} \ , \qquad (3.2)$$

где$k._{\text{зн.i}}$ – коэффициент значимости *i*-го фактора, $k._{\text{зн.i}}$ – коэффициент достигнутого уровня для *i*-го фактора.

Поскольку научно-исследовательская работа по исследованию методов и подходов совместной передачи классических оптических импульсов и квантовых состоянийявляется поисковой, произведем для нее расчет коэффициентов *научной* и *научно-технической* результативности. Оценка исследования приведена в таблице 6.

Таблица 6 – Оценка научной и научно-технической результативности прикладных исследований

Фактор научной результативности	Коэффициент значимости фактора	Качество фактора	Коэффициент достигнутого уровня
Факторы научной результативности			
Новизна результатов	0,5	Высокая	1,0
Глубина научной проработки	0,35	Высокая	1,0
Степень вероятности успеха	0,15	Умеренная	0,6
Факторы научно-технической результативности			
Перспективность использования результатов	0,5	Важная	0,8
Масштаб возможной реализации результатов	0,3	Отдельное предприятие (до 3-х лет)	0,4
Завершенность полученных результатов	0,2	Средняя	0,6

Исходя из данных таблицы 6, получим:

$$k_{\text{н.р.}} = 0{,}5 \cdot 1 + 0{,}35 \cdot 1 + 0{,}15 \cdot 0{,}6 = 0{,}94 \quad (3.3)$$

$$k_{\text{нт.р.}} = 0{,}5 \cdot 0{,}8 + 0{,}3 \cdot 0{,}4 + 0{,}2 \cdot 0{,}6 = 0{,}64 \quad (3.4)$$

При расчёте коэффициента научной результативности было получено значение 0,94, что говорит о высокой научной значимости работы. Коэффициент научно-технической результативности 0,64 указывает на возможность использования проведенных исследований в других НИР, а также в процессе производства новой продукции.

Различают три вида экономического эффекта научно-исследовательской работы:

- предварительный;
- ожидаемый;
- фактический.

Предварительный экономический эффект устанавливается при обосновании темы научного исследования и включении ее в план работ. Рассчитывают его по ориентировочным, укрупненным показателям с учетом прогнозируемого объема внедрения результатов исследований в группу предприятий данной отрасли.

Ожидаемый экономический эффект вычисляют в процессе выполнения НИР. Его условно относят (прогнозируют) к определенному периоду (году) внедрения продукции в производство.

Фактический экономический эффект определяется после внедрения научных разработок в производство, но не ранее, чем через год. Расчет его производят по фактическим затратам на научные исследования и внедрение с учетом конкретных стоимостных показателей данной отрасли (предприятия), где внедрены научные разработки.

Количественным показателем ожидаемого, либо фактического экономического эффекта является ожидаемая, либо фактическая экономия (Э), которая определяется по формуле:

$$Э = ЗПР_2 - ЗПР_1, \quad (3.5)$$

где $ЗПР_2$ и $ЗПР_1$ – приведенные затраты соответственно старого (базовый вариант) и нового варианта (на основе результатов научных исследований) соответственно.

Приведенные затраты рассчитываются по выражению:

$$ЗПР_1 = С + Е_н \cdot К, \quad (3.6)$$

где С – себестоимость единицы продукции, руб; $Е_н$ – нормативный коэффициент экономической эффективности (равный 0,15); К – капитальные вложения на создания новой технической продукции, руб.

Проведенные исследования методов и подходов совместной передачи классических оптических импульсов и квантовых состояний могут быть использованы при производстве при производстве аппаратуры квантового распределения ключей, допускающей работу на существующей инфраструктуре ВОЛС и/или детекторов одиночных фотонов (ДОФ) как самостоятельного изделия.

Для разворачивания комплексов по защите информации на основе аппаратуры КРК требуется отдельное темное волокно между объектами защиты, оснащенными модулями аппаратуры КРК, для создания квантового канала. Существующая инфраструктура ВОЛС уже перегружена и редко можно встретить резервные темные волокна. Затраты на прокладку новых ВОЛС составляют сотни миллионов рублей на оптоволоконные кабели, не считая стоимость сопутствующих работ.

Для уплотнения каналов передачи данных используются технологии спектрального уплотнения по длине волны в оптическом волокне. Возможность использования существующей инфраструктуры ВОЛС для реализации квантового канала с помощью технологии мультиплексирования позволит уже сейчас использовать аппаратуру КРК для защиты данных критической инфраструктуры, позволяя сэкономить значительные финансовые средства.

Для расчета приведенных затрат на новый вариант продукции необходимо определить капитальные вложения. Будем считать, что они определяются затратами на проведение научно исследовательской работы, которые складываются из расходов на оплату труда инженеров-исследователей, отчисления на социальные нужды, прочие расходы.

Затраты на основную заработную плату ($З_{о.з.п.и}$) исполнителя исследования определяются умножением размера месячной стипендии на число месяцев, отводимых на выполнение квалификационной работы:

$$З_{о.з.п.и.} = 4200 \cdot 5 = 21000 \text{руб.} \quad (3.7)$$

Основная заработная плата руководителя дипломной работы ($З_{о.з.п.р.}$) определяется исходя из суммарной нормы затрат рабочего времени в днях на одну дипломную работу (20 дней) и среднечасовой заработной платы исходя из оклада в 30000 рублей:

$$З_{о.з.п.р.} = 20 \cdot 16 \cdot 90 = 28800 \text{ руб.} \quad (3.8)$$

Руководителю начисляется дополнительная заработная плата ($З_{д.з.п.р}$), составляющая 12% от основной:

$$З_{д.з.п.р.} = 28800 * 0{,}12 = 3456 \text{ руб.} \quad (3.9)$$

Отчисления на социальное страхование ($З_{с.с}$) принимаются в размере 34% от суммы основной и дополнительной заработной платы:

$$З_{с.с.} = 32256 \cdot 0{,}34 = 10967{,}04 \text{ руб.} \quad (3.10)$$

Прочие расходы определяются платой за услуги привлеченного квалифицированного персонала (10000 руб), услуги консультантов (3500 руб).

Общая смета затрат на проведение научно-исследовательской работы представлена в таблице 7.

Таблица 7 – Смета затрат на проведение научно-исследовательской работы

№ п/п	Наименование статей затрат	Сумма, руб.
	Заработная плата:	
1	исполнителя исследования	21 000,00
2	Руководителя	32 256,00
3	Отчисления на социальное страхование	10 967,04
	Прочие расходы:	
4	услуги привлеченного квалифицированного персонала	10 000,00
5	услуги консультантов	3 500,00
Себестоимость НИР		77 723,04

Рассчитаем ожидаемый экономический эффект исследования методов и подходов совместной передачи классических оптических импульсов и квантовых состояний при разворачивании одной установки аппаратуры КРК на линии длиной 50 км. Стоимость 1 км волоконно-оптического кабеля составляет 2 978,00 рублей, тогда затраты на 50 км составят 148 900,00 рублей. Без учета стоимость работ по прокладке экономия составит:

$$Э = С - 0.15 \cdot 77723,04 = C - 11658,45 = 137241,55 \qquad (3.11)$$

Научно-исследовательская работа по исследованию методов и подходов совместной передачи классических оптических импульсов и квантовых состояний имеет как научный, научно-технический так и экономический эффект.

Исследование может быть применено при производстве аппаратуры КРК, адаптированной к работе на существующей инфраструктуре ВОЛС без выделения отдельного темного волокна.

ЗАКЛЮЧЕНИЕ

Проанализированы существующие методы и подходы совместной передачи классических оптических импульсов и квантовых состояний. Акцент сделан на технические решения, обеспечивающие адаптацию аппаратуры квантового распределения ключей (КРК) к её использованию на инфраструктуре существующих оптических транспортных сетей.

Основным решением данной задачи выбран метод мультиплексирования с разделением по длине волны оптических сигналов, который обеспечивает совместную передачу классических и квантовых сигналов в одном оптическом волокне.

Для адаптации аппаратуры КРК к совместной работе на инфраструктуре существующих оптических транспортных сетей особо выделен детектор одиночных фотонов (ДОФ). Модернизация ДОФ позволит уменьшить негативные последствия использования засвеченных оптических волокон для передачи квантовых состояний. Сформулированы дополнительные требования к ДОФ.

Проанализированы существующие типы оптических детектирующих элементов, способных регистрировать оптическое излучение на телекоммуникационных длинах волн с энергией, сопоставимой с энергией одиночного фотона. Выбор сделан в пользу малогабаритного однофотонного лавинного фотодиода, обеспечивающего достаточную квантовую эффективность при допустимом уровне темновых шумов.

Разработан концепт адаптированного ДОФ, включающий в себя:

– перечень функциональных блоков ДОФ с описанием их функционирования и предъявляемым техническим характеристикам;

– описание структуры функциональных блоков ДОФ с выделением основных структурных элементов;

– описание режимов работы ДОФ, включающих режим инициализации, режим ожидания и рабочий режим;

– описание процедур конфигурирования, калибровки и самодиагностики ДОФ.

Подсистема защиты ДОФ от ослепления мощным (многофотонным) оптическим излучением, подаваемым на оптический вход, реализована в блоке питания ОЛФД высокого напряжения. Мониторинг тока, протекающего через ОЛФД, позволяет отследить момент перехода в линейный режим, свидетельствующий о внешнем нештатном воздействии на ОЛФД через оптический вход. Механизмы противодействия включают снятие питающего высокого напряжения. Повторный переход в линейный режим после восстановлении питающего высокого напряжения свидетельствует о невозможности выполнения ДОФ своих функций, и сопровождается формированием команды в сопряженное устройство о функциональной ошибке.

Взаимодействие ДОФ с ПЭВМ или в рамках аппаратуры КРК происходит посредством команд с помощью канала связи, подключаемого к процессору ПЛИС. При работе ДОФ с ПЭВМ используется системное программное обеспечение (СПО), предоставляемое разработчиком ДОФ. СПО позволяет пользователю взаимодействовать с ДОФ, а также выполнять первичную обработку результатов измерения.

Разработанный концепт ДОФимеет технические характеристики на уровне лучших аналогов и удовлетворяет требованиям по защите от ослепления для возможности его использования в аппаратуре КРК, работающей на инфраструктуре существующих волоконно-оптических линий связи.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] *D. Townsend Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelengthdivision multiplexing // Electronics Letters. 1997. vol. 33. no. 3. pp. 188–190.*

[2] *N. Nweke, P. Toliver, R. Runser, S. McNown, J. Khurgin, T. Chapuran, M. Goodman, R. Hughes, C. Peterson, K. McCabe et al., Experimental characterization of the separation between wavelength-multiplexed quantum and classical communication channels // Applied Physics Letters. 2005. vol. 87. no. 17. p. 174103.*

[3] *R. J. Runser, T. Chapuran, P. Toliver, N. A. P., M. S. Goodman, J. T. K., N. Nweke, S. R. McNown, R. J. Hughes, D.Rosenberg, C. G. Peterson, K. P. McCabe, J. E. Nordholt, K. Tyagi, P. A. Hiskett Nicholas Dallmann Progress Toward Quantum Communications Networks: Opportunities and Challenges // Proc. SPIE 6476. Optoelectronic Integrated Circuits IX. 2007. p. 64760I*

[4] *T.E. Chapuran, P. Toliver, N.A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes , K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer and H. Dardy Optical networking for quantum key distribution and quantum communications // New Journal of Physics. 2009. V. 11. P. 105001.*

[5] *P. Eraerds, N. Walenta, M. Legr´e, N. Gisin, and H. Zbinden Quantum key distribution and 1 gbps data encryption over a single fibre // New Journal of Physics. 2010. vol. 12. no. 6. p. 063027.*

[6] *Iris Choi, Robert J. Young and Paul D. Townsend Quantum key distribution on a 10Gb/s WDM-PON // Optics Express. 2010. Vol. 18. No. 9. P. 9601.*

[7] *K. A. Patel J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon,1 Z. L. Yuan, R. V. Penty and A. J. Shields Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber // PHYS. REV. X. 2012. V. 2. P. 041010.*

[8] *J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. García Muñoz, and J. Capmany Simultaneous transmission of 20x2 WDM/SCMQKD and 4 bidirectional classical channels over a PON // Optics Express. 2012. Vol. 20. No. 15. P. 16358.*

[9] *K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty and A. Shields Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks // Applied Physics Letters. 2014. vol. 104 no. 5. p. 051123.*

[10] *Rupesh Kumar, Hao Qin and Romain Alléaume Coexistence of continuous variable QKD with intense DWDM classical channels // New J. Phys. 2015. V. 17. P. 043027.*

[11] *J. F. Dynes, W. W-S. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards & A. J. Shields Ultra-high*

bandwidth quantum secured data transmission // Scientific Reports. 2016. vol. 6. p. 35149.

[12] *L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen et al. Long-distance copropagation of quantum key distribution and terabit classical optical data channels // Physical Review A. 2017. vol. 95. no. 1. p. 012301.*

[13] *Yingqiu Mao, Bi-Xiao Wang, Chunxu Zhao, Guangquan Wang, Ruichun Wang, Honghai Wang, Fei Zhou, Jimin Nie, Qing Chen, Yong Zhao, Qiang Zhang, Jun Zhang, Teng-Yun Chen, and Jian-Wei Pan Integrating quantum key distribution with classical communications in backbone fiber network // Optics Express. 2018. V. no. 5. P. 6010.*

[14] *C. Cai, Y. Sun, Y. Zhang, P. Zhang, J. Niu, and Y.g Ji Experimental wavelength-space division multiplexing of quantum key distribution with classical optical communication over multicore fiber // Optics Express. 2019. vol. 27. no. 4. pp. 5125-5135.*

[15] *Tobias A. Eriksson, Takuya Hirano, Benjamin J. Puttnam, Georg Rademacher, Ruben S. Luís, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada & Masahide Sasaki Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels // Communications Physics. V. 2. No. 9. P. 1.*

[16] *S. Wengerowsky, S.K. Joshi, F. Steinlechner, H. Hübe., R. Ursin An entanglement-based wavelength-multiplexed quantum communication network // Nature. 2018. vol. 564. pp. 225-233.*

[17] *D. Aktas, B. Fedrici, F. Kaiser, T. Lunghi, L. Labont´e, and S. Tanzilli Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography // Laser Photonics Rev. 2016. vol. 10. no. 3. pp. 451–457.*

[18] *Fukasawa, A., Haba, J., Kageyama, A., Nakazawa, H. & Suyama, M. High speed HPD for photon counting. IEEE Trans. Nucl. Sci. 55, 758–762 (2008).*

[19] *Eraerds, P., Legré, M., Rochas, A., Zbinden, H. & Gisin, N. SiPM for fast photon-counting and multiphoton detection. Opt. Express 15, 14539–14549 (2007)*

[20] *Bethune, D. S. & Risk, W. P. An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. IEEE J. Quant. Elect. 36, 340–347 (2000).*

[21] *Pellegrini S. et al. Design and performance of an InGaAs-InP single-photon avalanche diode detector. IEEE J. Quant. Elect. 42, 397–403 (2006).*

[22] *Waks, E. et al. High-efficiency photon-number detection for quantum information processing. IEEE J. Sel. Top. Quant. 9, 1502–1511 (2003)*

[23] *Miller, A. J., Nam, S. W., Martinis, J. M. & Sergienko, A. V. Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination. Appl. Phys. Lett. 83, 791–793 (2003)*
[24] *Rosenberg, D., Lita, A. E., Miller, A. J. & Nam, S. W. Noise-free high-efficiency photon-number-resolving detectors. Phys. Rev. A 71, 061803 (2005).*
[25] *Lita, A. E., Miller, A. J. & Nam, S. W. Counting near-infrared single-photons with 95% efficiency. Opt. Express 16, 3032–3040 (2008).*
[26] *Fukuda, D. et al. Photon number resolving detection with high speed and high quantum efficiency. Metrologia 46, S288–S292 (2009)*
[27] *Gol'tsman, G. N. et al. Picosecond superconducting single-photon optical detector. Appl. Phys. Lett. 79, 705–707 (2001).*
[28] *Il'in, K. S. et al. Picosecond hot-electron energy relaxation in NbN superconducting photodetectors. Appl. Phys. Lett. 76, 2752–2754 (2000).*
[29] *Verevkin, A. et al. Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range. Appl. Phys. Lett. 80, 4687–4689 (2002).*
[30] *Miki, S. et al. Large sensitive-area NbN nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates. Appl. Phys. Lett. 92, 061116 (2008).*
[31] *Kerman, A. J. et al. Constriction-limited detection efficiency of superconducting nanowire single-photon detectors. Appl. Phys. Lett. 90, 101110 (2007).*
[32] *Kerman, A. J. et al. Kinetic-inductance-limited reset time of superconducting nanowire photon counters. Appl. Phys. Lett. 88, 111116 (2006).*
[33] *Hadfield, R. H. et al. Single photon source characterization with a superconducting single photon detector. Opt. Express 13, 10846–10853 (2005).*
[34] *Rosfjord, K. M. et al. Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating. Opt. Express 14, 527–534 (2006).*
[35] *Shields, A. J. Semiconductor quantum light sources. Nature Photon. 1, 215–223 (2007).*
[36] *Rowe, M. A. et al. Single-photon detection using a quantum dot optically gated field-effect transistor with high internal quantum efficiency. Appl. Phys. Lett. 89, 253505 (2006).*
[37] *Kardynal, B. E. et al. Photon number resolving detector based on a quantum dot field effect transistor. Appl. Phys. Lett. 90, 181114 (2007).*
[38] *Kosaka, H. et al. Photoconduction quantization in a single-photon detector. Phys. Rev. B 65, 201307 (2002)*
[39] *Kardynał, B. E. et al. Low-noise photon counting with a radio-frequency quantum-dot field-effect transistor. Appl. Phys. Lett. 84, 419–421 (2004)*

[40] *Li, H. W. et al. Quantum dot resonant tunneling diode for telecommunication wavelength single photon detection. Appl. Phys. Lett. 91, 073516 (2007)*
[41] *Gobby, C., Yuan, Z. L. & Shields, A. J. Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. 84, 3762–3764 (2004)*
[42] *Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. Opt. Express 16, 18790–18797 (2008).*
[43] *Takesue, H. et al. Quantum key distribution over 40-dB channel loss using superconducting single-photon detectors. Nature Photon. 1, 343–348 (2007)*
[44] *Blakesley, J. C. et al. Efficient single photon detection by quantum dot resonant tunneling diodes. Phys. Rev. Lett. 94, 067401 (2005).*
[45] К. А. Балыгин, В. И. Зайцева, А. И. Климова, А. Н. Климовb, С. П. Куликb, С. Н. Молотков Модуль регистратора однофотонных сигналов. Приборы и техника эксперимента, 2018, №4, (стр 1–6).
[46] В. В. Преображенский, И. Б. Чистохин, М. А. Путято, Н. А. Валишева, Е. А. Емельянов, М. О. Петрушков, А. С. Плешков, И. Г. Неизвестный, И. И. Рябцев Детекторы одиночных фотонов на основе лавинных фотодиодов InP/InGaAs/InP // АВТОМЕТРИЯ. 2021. Т. 57, № 5
[47] *Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov Hacking commercial quantum cryptography systems by tailored bright illumination //Nature Photonics, october 2010*
[48] *C Wiechers, L Lydersen, C Wittmann, D Elser, J Skaar, Ch Marquardt, V Makarov and G Leuchs After-gate attack on a quantum cryptosystem // New Journal of Physics 13 (2011)*
[49] *Polina Acheva, Konstantin Zaitsev, Vladimir Zavodilenko, AntonLosev, Anqi Huang and Vadim Makarov Automated verification of countermeasure against detector-control attack in quantum key distribution // EPJ Quantum Technology https://doi.org/10.1140/epjqt/s40507-023-00178-x*
[50] *Nitin Jain, Elena Anisimova, Imran Khan, Vadim Makarov, Christoph Marquardt and Gerd Leuchs Trojan-horse attacks threaten the security of practical quantum cryptography // New Journal of Physics 16 (2014)*
[51] *Ilja Gerhardt, Qin Liu, Antнa Lamas-Linares, Johannes Skaar, Christian Kurtsiefer & Vadim Makarov Full-field implementation of a perfect eavesdropper on a quantum cryptography system //Nature Communications, 2011*

«УТВЕРЖДАЮ»
Заведующий кафедрой НиМЭ
Пронин И.А.
(фамилия, инициалы)
«22» мая 2024 г.

З А Д А Н И Е
на выпускную квалификационную работу магистра

1. Студент гр. 22ПДм1 факультета ФИТЭ
Направление подготовки 11.04.04 «Электроника и наноэлектроника»
Магистерская программа Нано- и микроэлектроника
Филиппов Алексей Викторович
(фамилия, инициалы)

2. Руководитель Карманов А.А.
(фамилия, инициалы)

3. Тема выпускной квалификационной работы: «Разработка методов и подходов совместной передачи классических оптических импульсов и квантовых состояний»
Тема утверждена приказом ПГУ № 1059/о от «30» ноября 2022 г.

4. Техническое задание на выпускную работу работу (разработать, исследовать (назначение объекта разработки, исследования), исходные данные, граничные условия разрабатываемого или исследуемого объекта, условия эксплуатации и т.д.)
4.1. исследовать существующие методы и подходы совместной работы квантовых и классических каналов в одном оптическом волокне;
4.2. разработать методы организации квантовых и классических каналов в рамках одного оптического волокна на основе мультиплексирования по длине волны;
4.3. определить параметры передачи и структурные элементы аппаратуры квантового распределения ключей для совместной передачи квантовых и классических сигналов;
4.4. разработать предложения по доработке структурных элементов, обеспечивающие улучшенные ТТХ при совместной передаче квантовых и классических сигналов;
4.5. разработать концепт детектора одиночных фотонов, адаптированный под совместную передачу квантовых и классических сигналов.

5. Объем и содержание основной части выпускной работы
5.1. Пояснительная записка (перечень вопросов, подлежащих разработке, обоснований, описаний, расчетов и т.д.)
1 Теоретические основы совместной передачи классических и квантовых сигналов в одном волокне
1.1 Анализ источников по совместной передаче классических и квантовых сигналов в одном оптическом волокне
1.2 Подходы и методы эффективной совместной передачи квантовых и информационных оптических сигналов в одном оптическом волокне
1.3 Адаптация аппаратуры КРК

1.4 Тактико-технические характеристики ДОФ
1.5 Выбор типа чувствительного элемента ДОФ
1.6 Описание принципов работы ДОФ на основе ОЛФД
1.7 Адаптация ДОФ к работе в общих оптических сетях
2 Экспериментальная работа по моделированию совместной передачи классических и квантовых сигналов в одном волокне
2.1 Структурная схема адаптированного ДОФ
2.2 Параметры конфигурации ДОФ
2.3 Алгоритм работы ДОФ
2.4 Обработка и передача результатов измерения
3 Расчет экономической эффективности

5.2. Иллюстративная часть (перечень и название слайдов презентации)

1. Титульный слайд (слайд №1)
2. Цели и задачи работы (слайд №2)
3. Каналы связи аппаратуры КРК (слайд №3)
4. Методы совместной передачи классических и квантовых сигналов (слайд №4, 5)
5. Мультиплексирование классических и квантовых сигналов по длине волны (слайд №6)
6. Адаптация аппаруты КРК под совсместную передачу в одном волокне (слайд №7)
7. Тактико-технические характеристики адаптированного ДОФ (слайд №8)
8. ДОФ на основе однофотонного лавинного фотодида (слайд №9)
9. Структурная схема ДОФ (базовая схем включения) (слайд №10)
10. Структурная схема ДОФ (разрабатываемый концепт) (слайд №11)
11. Адаптация ДОФ (управляемый прямоугольный строб) (слайд №12)
12. Адаптация ДОФ (активное гашение лавины) (слайд №13)
13. Адаптация ДОФ (защита от неконтролируемой засветки) (слайд №14)
14. Основные выводы (слайд №15)

6. Консультанты и содержание дополнительных разделов (по технологии, по экологии, по экономике, по безопасности жизнедеятельности, по этике, и т.д. Указывается конкретное содержание задания)

6.1.

Консультант

7. Календарный план по выполнению выпускной работы магистра

Наименование этапов работы	Объем работы	Срок выполнения	Подпись руководителя
Теоретические основы совместной передачи классических и квантовых сигналов в одном волокне	30%	23.05.2024	
Экспериментальная работа по моделированию совместной передачи классических и квантовых сигналов в одном волокне	35%	25.05.2024	
Расчет экономической эффективности	10%	27.05.2024	
Иллюстративная часть	15%	28.05.2024	
Оформление пояснительной записки	10%	01.06.2024	

Руководитель выпускной работы _____ Карманов А.А.
(подпись) (фамилия, инициалы)

Дата выдачи задания «22» мая 2024 г.

Задание к исполнению принял _____ Филиппов А.В.
(подпись) (фамилия, инициалы)

«22» мая 2024 г.

Выпускную квалификационную работу к защите допустить

Декан факультета _____ Кревчик В.Д.
(подпись) (фамилия, инициалы)

«10» 06 2024 г.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 792 414** (13) **C1**

(51) МПК
H04L 9/08 (2006.01)
(52) СПК
H04L 9/08 *(2023.02)*
G06F 21/72 *(2023.02)*

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

Статус: действует (последнее изменение статуса: 27.03.2023)
Пошлина: Установленный срок для уплаты пошлины за 3 год: с 29.06.2023 по 28.06.2024. При уплате пошлины за 3 год в дополнительный 6-месячный срок с 29.06.2024 по 28.12.2024 размер пошлины увеличивается на 50%.

(21)(22) Заявка: **2022117367, 28.06.2022**

(24) Дата начала отсчета срока действия патента:
28.06.2022

Дата регистрации:
22.03.2023

Приоритет(ы):
(22) Дата подачи заявки: **28.06.2022**

(45) Опубликовано: **22.03.2023** Бюл. № **9**

(56) Список документов, цитированных в отчете о поиске: **RU 2708511 C1, 09.12.2019. RU 2621605 C2, 06.06.2017. RU 2764458 C1, 17.01.2022. RU 2697696 C1, 16.08.2019. US 2018/0191496 A1, 05.06.2018.**

Адрес для переписки:
440026, г. Пенза, ул. Лермонтова, 3, ООО НТП "Криптософт", Водневу А.В.

(72) Автор(ы):
Филиппов Алексей Викторович (RU),
Букин Евгений Геннадьевич (RU),
Карманов Андрей Андреевич (RU)

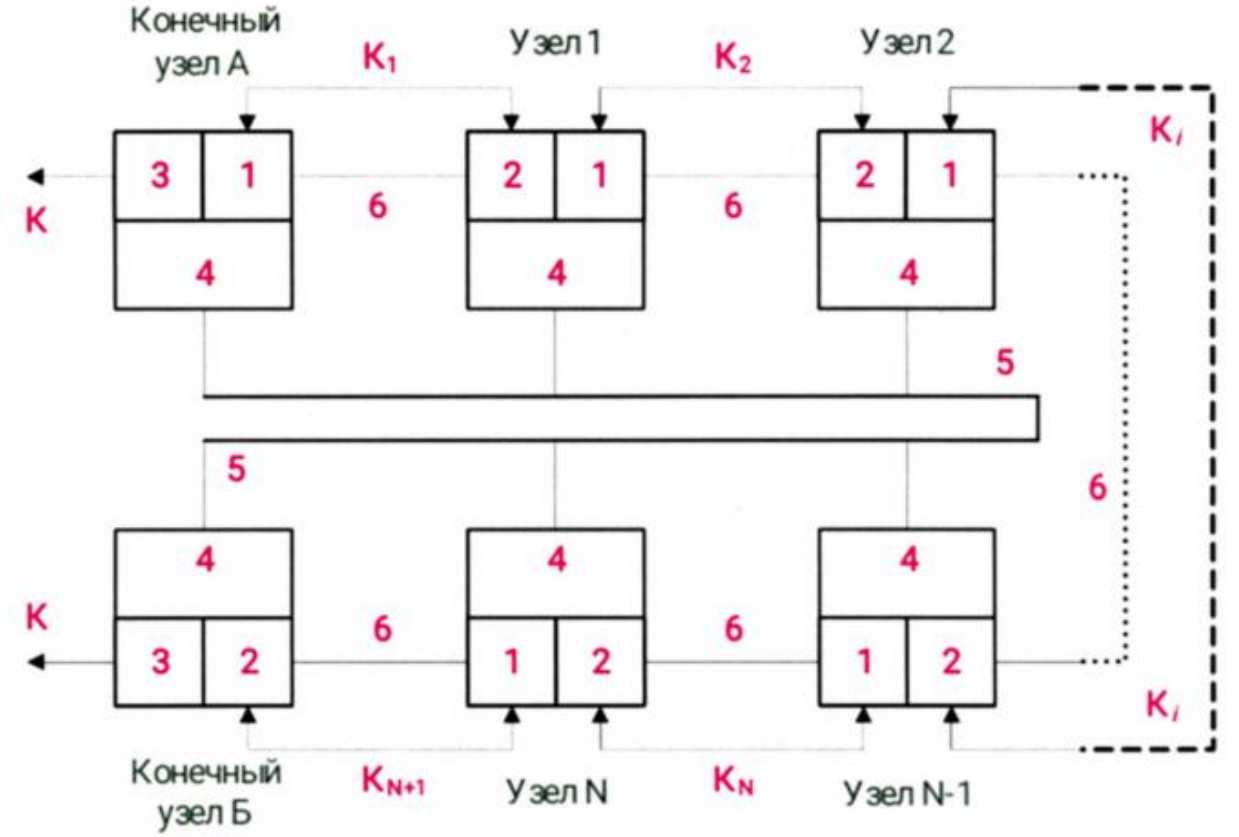
(73) Патентообладатель(и):
Общество с ограниченной ответственностью научно-техническое предприятие "Криптософт" ООО НТП "Криптософт" (RU)

(54) СПОСОБ ПЕРЕДАЧИ ИНФОРМАЦИИ МЕЖДУ КОНЕЧНЫМИ УЗЛАМИ СВЯЗИ ЧЕРЕЗ ПРОМЕЖУТОЧНЫЕ УЗЛЫ БЕЗ ПЕРЕШИФРОВАНИЯ

(57) Реферат:

Изобретение относится к области обеспечения защиты передаваемой информации. Технический результат заключается в обеспечении возможности защищенной передачи информации между конечными узлами через промежуточные узлы связи с высокой скоростью и отсутствием ограничений на применяемые криптографические алгоритмы защиты информации. Способ включает выработку локальных ключей K_i между смежными узлами, i=1, 2, …, N+1, где N - число промежуточных узлов. Согласно изобретению модуль криптографической защиты промежуточного узла, имея локальные ключи K_i и K_{i+1}, выработанные со смежными узлами, подготавливает и отправляет два сообщения для конечных узлов А и Б, причем в первом сообщении для конечного узла А ключ K_{i+1} зашифрован на ключе K_i, во втором сообщении для конечного узла Б ключ K_i зашифрован на ключе K_{i+1}. После получения сообщений от всех промежуточных узлов и расшифрования их содержимого конечные узлы имеют одинаковый набор локальных ключей $\{K_1, K_2, \ldots, K_N, K_{N+1}\}$ и далее, используя функцию F, формируют общий ключ К для защищенной связи между конечными

узлами. 1 з.п. ф-лы, 1 ил.



Фиг. 1

РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 817 659** (13) **C2**

(51) МПК
H04L 9/08 (2006.01)
(52) СПК
H04L 9/08 *(2023.08)*
H04L 9/0855 *(2023.08)*

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

Статус: действует (последнее изменение статуса: 20.04.2024)
Пошлина: Установленный срок для уплаты пошлины за 3 год: с 21.07.2023 по 20.07.2024. При уплате пошлины за 3 год в дополнительный 6-месячный срок с 21.07.2024 по 20.01.2025 размер пошлины увеличивается на 50%.

(21)(22) Заявка: **2022119942, 20.07.2022**

(24) Дата начала отсчета срока действия патента:
20.07.2022

Дата регистрации:
17.04.2024

Приоритет(ы):
(22) Дата подачи заявки: **20.07.2022**

(43) Дата публикации заявки: **22.01.2024** Бюл. № 3

(45) Опубликовано: **17.04.2024** Бюл. № 11

(56) Список документов, цитированных в отчете о поиске: **RU 2752844 C1, 11.08.2021. RU 2737105 C1, 24.11.2020. US 20160248581 A1, 25.08.2016. CN 101742496 A, 16.06.2010. US 20160013936 A1, 14.01.2016.**

Адрес для переписки:
440026, г. Пенза, ул. Лермонтова, 3, ООО НТП "Криптософт", генеральному директору Вартанову Артуру Александровичу

(72) Автор(ы):
Филиппов Алексей Викторович (RU),
Букин Евгений Геннадьевич (RU),
Карманов Андрей Андреевич (RU)

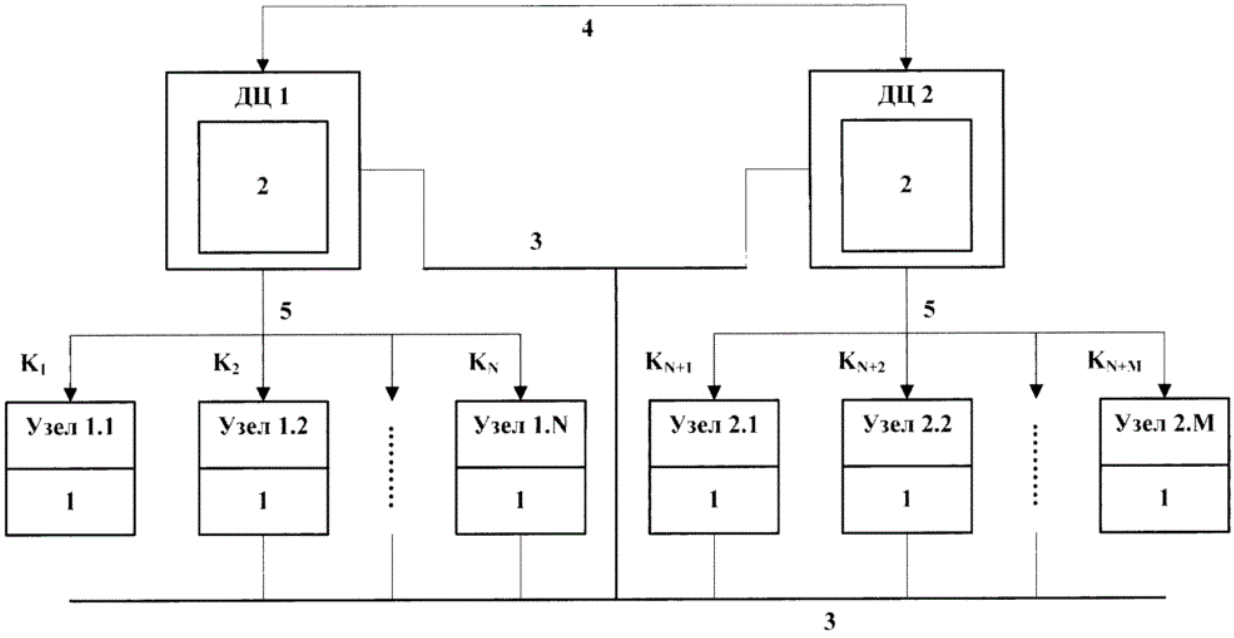
(73) Патентообладатель(и):
Общество с ограниченной ответственностью научно-техническое предприятие "Криптософт" ООО НТП "Криптософт" (RU)

(54) ДИНАМИЧЕСКАЯ СИСТЕМА ФОРМИРОВАНИЯ И РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ БЕЗ КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

(57) Реферат:

Изобретение относится к области защиты информации в сетях связи. Технический результат заключается в обеспечении возможности защищенной передачи информации между узлами связи как в рамках одной подсети, так и в рамках разных подсетей. Динамическая система формирования и распределения ключей без компрометации ключевой информации включает по меньшей мере две подсети, каждая из которых содержит доверенный центр с модулем формирования ключей, при этом каждый доверенный центр соединен локальным защищенным каналом, по меньшей мере, с одним узлом связи, а узлы связи соединены между собой общим транспортным каналом. Каждый узел связи содержит средство криптографической защиты информации, а все доверенные центры соединены между собой общим

защищенным каналом, а также общим транспортным каналом. 2 н. и 4 з.п. ф-лы, 1 ил.



Фиг. 1

Ректору Пензенского
государственного университета
А.Д. Гулякову
студента 2 курса ФИТЭ
очной формы обучения
Филиппова Алексея Викторовича

ЗАЯВЛЕНИЕ

Я, Филиппов Алексей Викторович, студент 2 курса очной формы обучения направления подготовки 11.04.04 Электроника и наноэлектроника, магистерская программа «Нано- и микроэлектроника» прошу провести проверку с использованием системы «Антиплагиат.ВУЗ» магистерской выпускной квалификационной работы на тему «Разработка методов и подходов совместной передачи классических оптических импульсов и квантовых состояний», выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования - програ043Смам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета

Подпись студента

04.06.2024
дата

ВКР представлена на проверку 05.06.2024

Руководитель ВКР _____ А.А. Карманов

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Разработка методов и подходов совместной передачи классических оптических импульсов и квантовых состояний», студента 2 курса А.В. Филиппова, направления подготовки 11.04.04 Электроника и наноэлектроника, магистерской программы «Нано- и микроэлектроника». Руководитель ВКР А.А. Карманов

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

СПРАВКА

Пензенский государственный университет

о результатах проверки текстового документа
на наличие заимствований

ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Филиппов Алексей Викторович
Самоцитирование рассчитано для: Филиппов Алексей Викторович
Название работы: Разработка методов и подходов совместной передачи классических оптических импульсов и квантовых состояний
Тип работы: Магистерская диссертация
Подразделение: Кафедра "Нано- и микроэлектроника"

РЕЗУЛЬТАТЫ

■ ОТЧЕТ О ПРОВЕРКЕ КОРРЕКТИРОВАЛСЯ; НИЖЕ ПРЕДСТАВЛЕНЫ РЕЗУЛЬТАТЫ ПРОВЕРКИ ДО КОРРЕКТИРОВКИ

СОВПАДЕНИЯ	12.45%	СОВПАДЕНИЯ	12.45%
ОРИГИНАЛЬНОСТЬ	86.83%	ОРИГИНАЛЬНОСТЬ	86.83%
ЦИТИРОВАНИЯ	0.72%	ЦИТИРОВАНИЯ	0.72%
САМОЦИТИРОВАНИЯ	0%	САМОЦИТИРОВАНИЯ	0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 05.06.2024 — ДАТА И ВРЕМЯ КОРРЕКТИРОВКИ: 05.06.2024 14:10

Модули поиска: Цитирование; ИПС Адилет; Переводные заимствования*; Библиография; СПС ГАРАНТ: нормативно-правовая документация; Шаблонные фразы; СПС ГАРАНТ: аналитика; Коллекция НБУ; Диссертации НББ; Патенты СССР, РФ, СНГ; IEEE; СМИ России и СНГ; Медицина; Сводная коллекция ЭБС; Публикации eLIBRARY; Публикации РГБ; Перефразирования по Интернету (EN); Кольцо вузов; Перефразирования по коллекции IEEE; Публикации eLIBRARY (переводы и перефразирования); Перефразирования по СПС ГАРАНТ: аналитика; Переводные заимствования по коллекции Интернет в английском сегменте; Перефразированные заимствования по коллекции Интернет в русском сегменте; Переводные заимствования по коллекции Интернет в русском сегменте; Переводные заимствования по Интернету (En-Ru); Переводные заимствования

Работу проверил: Голованькин Алексей Николаевич
ФИО проверяющего

Дата подписи:

Подпись проверяющего

Чтобы убедиться в подлинности справки, используйте QR-код, который содержит ссылку на отчет.

Отчет не вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

05.06.2024
дата

А.А. Карманов

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

Пензенский государственный университет

ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Филиппов Алексей Викторович
Самоцитирование рассчитано для: Филиппов Алексей Викторович
Название работы: Разработка методов и подходов совместной передачи классических оптических импульсов и квантовых состояний
Тип работы: Магистерская диссертация
Подразделение: Кафедра "Нано- и микроэлектроника"

РЕЗУЛЬТАТЫ

■ **ОТЧЕТ О ПРОВЕРКЕ КОРРЕКТИРОВАЛСЯ:** НИЖЕ ПРЕДСТАВЛЕНЫ РЕЗУЛЬТАТЫ ПРОВЕРКИ ДО КОРРЕКТИРОВКИ

СОВПАДЕНИЯ	12.45%		СОВПАДЕНИЯ	12.45%
ОРИГИНАЛЬНОСТЬ	86.83%		ОРИГИНАЛЬНОСТЬ	86.83%
ЦИТИРОВАНИЯ	0.72%		ЦИТИРОВАНИЯ	0.72%
САМОЦИТИРОВАНИЯ	0%		САМОЦИТИРОВАНИЯ	0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 05.06.2024

ДАТА И ВРЕМЯ КОРРЕКТИРОВКИ: 05.06.2024 14:10

Модули поиска: Цитирование; ИПС Адилет; Переводные заимствования*; Библиография; СПС ГАРАНТ: нормативно-правовая документация; Шаблонные фразы; СПС ГАРАНТ: аналитика; Коллекция НБУ; Диссертации НББ; Патенты СССР, РФ, СНГ; IEEE; СМИ России и СНГ; Медицина; Сводная коллекция ЭБС; Публикации eLIBRARY; Публикации РГБ; Перефразирования по Интернету (EN); Кольцо вузов; Перефразирования по коллекции IEEE; Публикации eLIBRARY (переводы и перефразирования); Перефразирования по СПС ГАРАНТ: аналитика; Переводные заимствования по коллекции Интернет в английском сегменте; Перефразированные заимствования по коллекции Интернет в русском сегменте; Переводные заимствования по коллекции Интернет в русском сегменте; Переводные заимствования по Интернету (EnRu); Переводные заимствования

Работу проверил: Головяшкин Алексей Николаевич

ФИО проверяющего

Дата подписи: 05.06.2024

Подпись проверяющего

Чтобы убедиться
в подлинности справки, используйте QR-код,
который содержит ссылку на отчет.

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Магистерская диссертация

«Разработка методов и подходов совместной передачи классических оптических импульсов и квантовых состояний»

Выполнил (группа 22ПДм1): Филиппов А.В.

Научный руководитель, к.ф-м.н.: Карманов А.А.

Цели и задачи работы

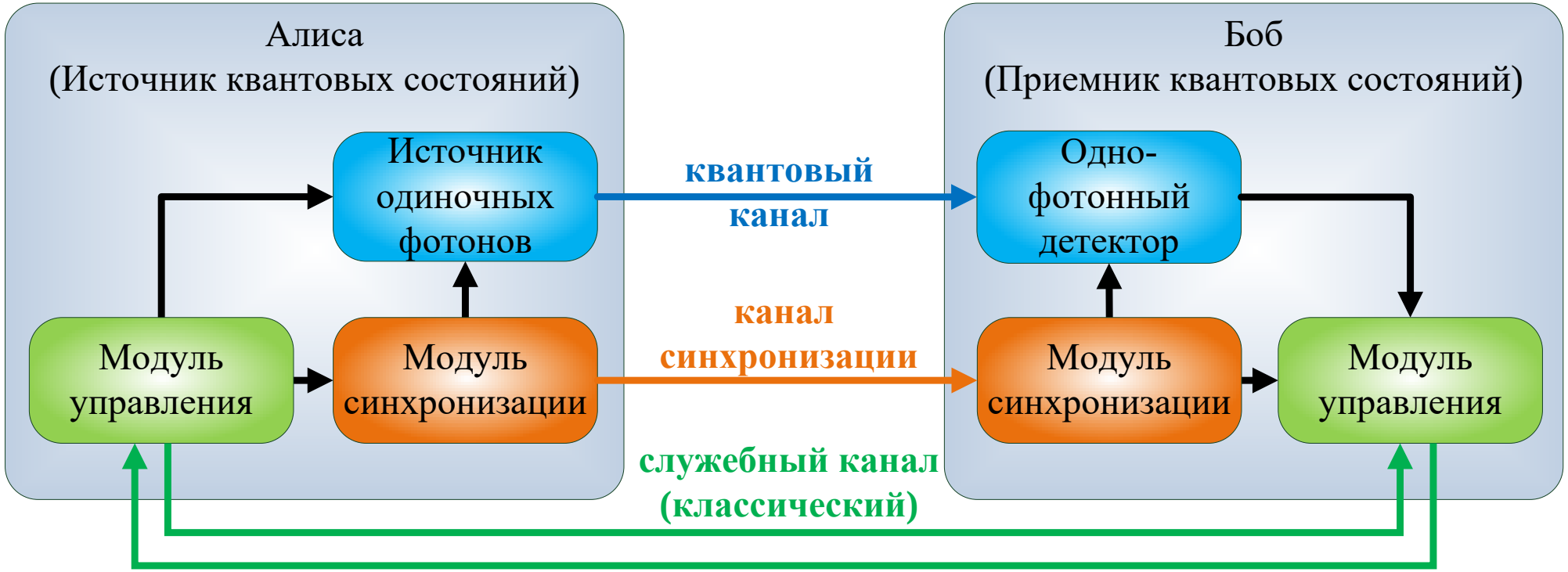
Цель:

- разработка подходов и методов совместного использования существующей инфраструктуры ВОЛС для передачи квантовых и классических сигналов в рамках одного оптического волокна при работе аппаратуры КРК с адаптированным детектором одиночных фотонов

Задачи:

- исследовать существующие методы и подходы совместной работы квантовых и классических каналов в одном оптическом волокне;
- разработать методы организации квантовых и классических каналов в рамках одного оптического волокна на основе мультиплексирования по длине волны
- определить параметры передачи и структурные элементы аппаратуры квантового распределения ключей для совместной передачи квантовых и классических сигналов
- разработать предложения по доработке структурных элементов, обеспечивающие улучшенные ТТХ при совместной передаче квантовых и классических сигналов
- разработать концепт детектора одиночных фотонов, адаптированный под совместную передачу квантовых и классических сигналов

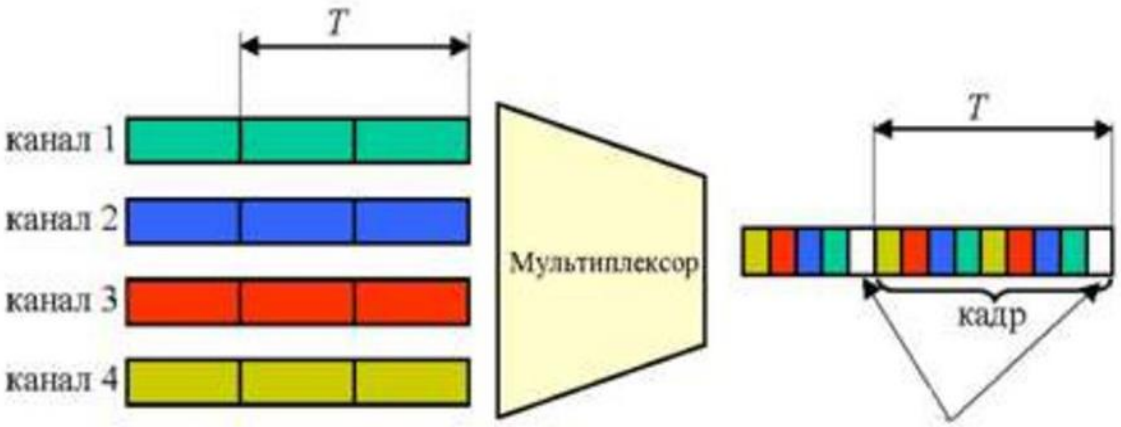
Каналы связи аппаратуры квантового распределения ключей

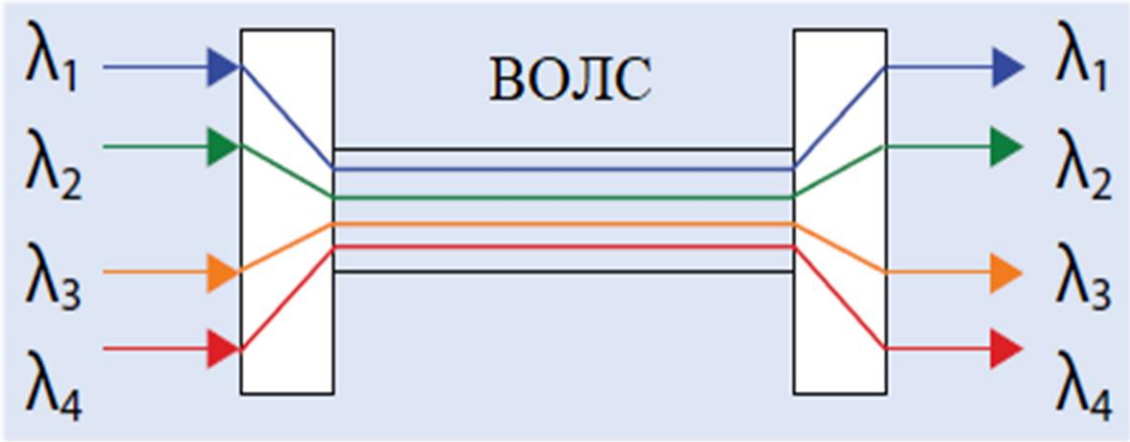


Основные каналы связи аппаратуры КРК:

- квантовый канал (передача одиночных фотонов)
- канал синхронизации (передача классических многофотонных сигналов)
- служебный канал (передача классических многофотонных сигналов)

Методы совместной передачи классических и квантовых оптических сигналов





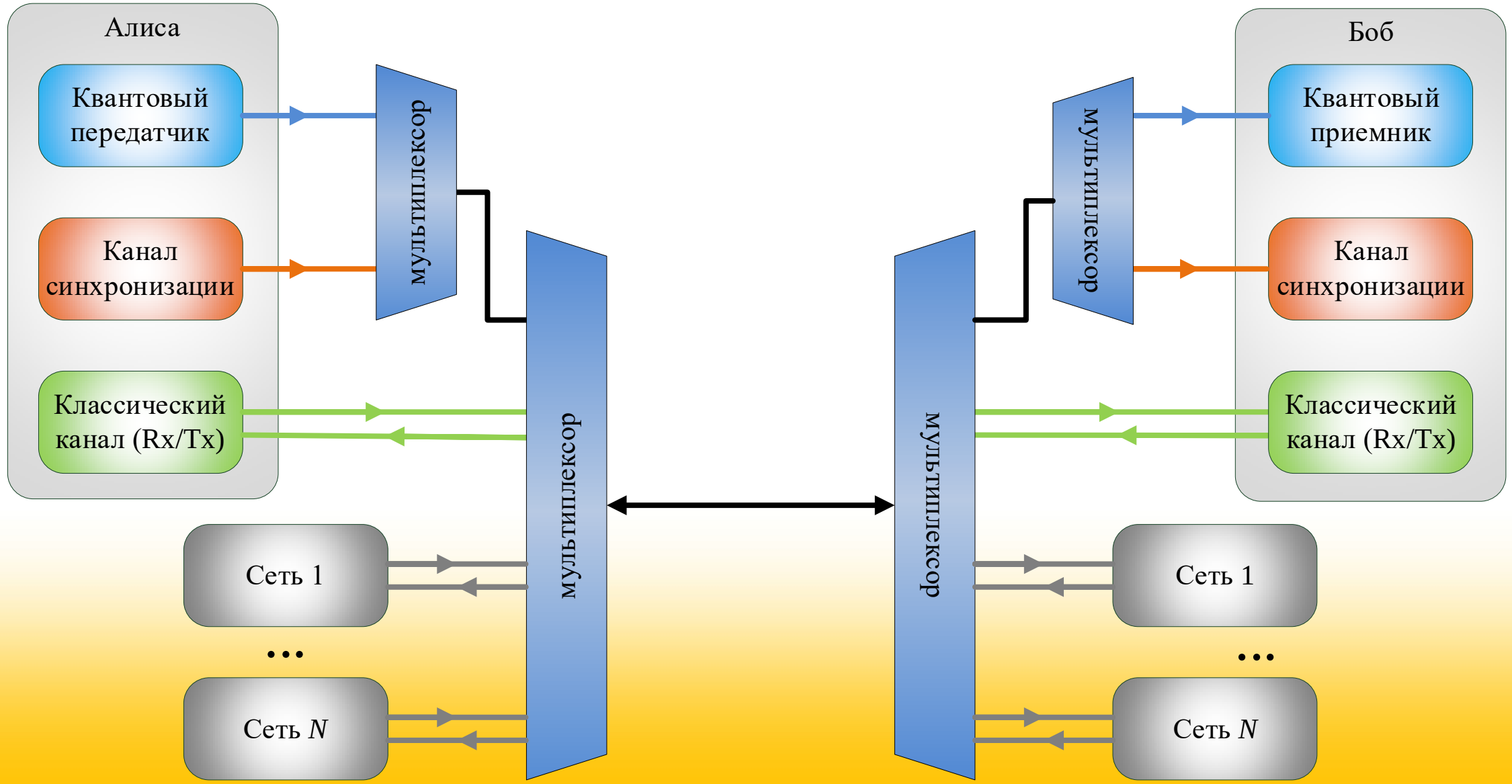
Мультиплексирование по времени

- каждому каналу предоставляется узкое временное окно
- все каналы должны иметь одинаковые характеристики
- не увеличивается пропускная способность оптической линии

Мультиплексирование по длине волны

- каждый канал работает на своей длине волны (параллельно)
- каналы независимы и могут быть любыми (по источнику излучения)
- увеличивается пропускная способность кратно числу каналов

Методы совместной передачи классических и квантовых сигналов



Мультиплексирование классических и квантовых сигналов по длине волны

Достоинства метода

- простота и надежность мультиплексора (пассивный оптический модуль)
- простота организации канала «подключил и забыл»
- отсутствие специфических требований к аппаратуре КРК и телекоммуникационному оборудованию

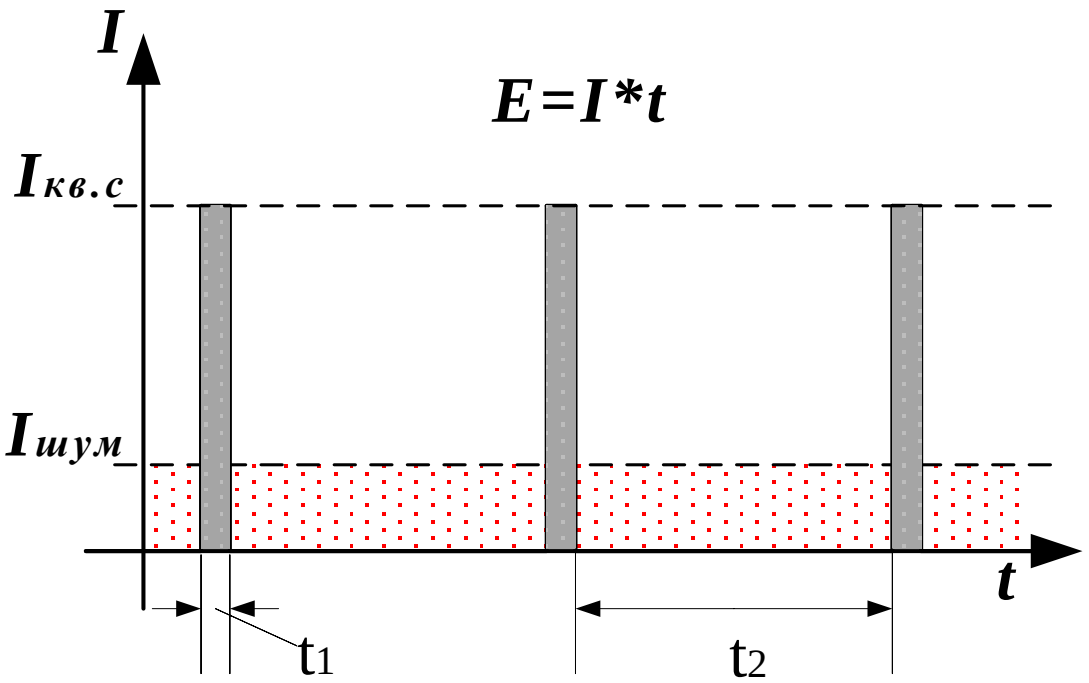
Недостатки метода

- зашумление квантового канала случайными вторичными фотонами:
  - увеличивает уровень ошибок в квантовом канале;
  - ограничивает дальность связи (длину квантового канала).

Зашумление квантового каналами случайными фотонами

- случайные шумовые фотоны генерируются атомами оптического волокна
- шумовые фотоны вызваны нелинейными оптическими процессами в оптическом волокне
- количество шумовых фотонов пропорционально мощности и количеству классических каналов

Адаптация аппаратуры КРК под совместную передачу



Структурные элементы квантового канала

ИОФ (источник одиночных фотонов)

- уменьшение времени импульса
- сужение спектра излучения

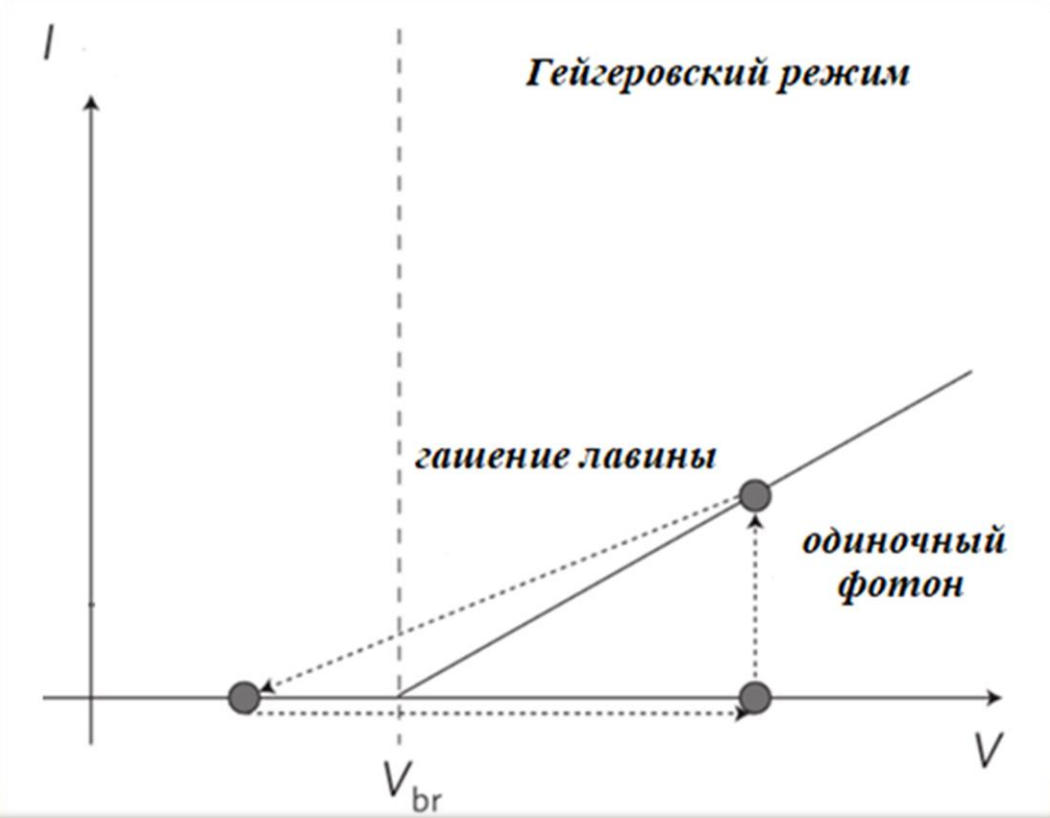
ДОФ (детектор одиночных фотонов)

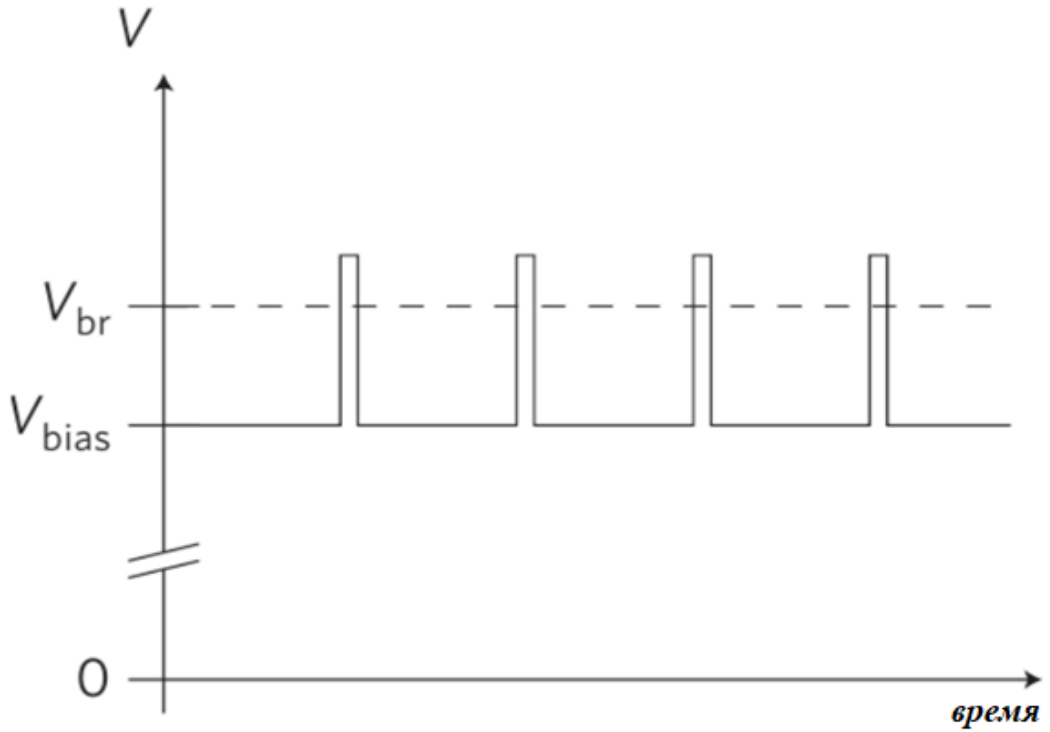
- уменьшение длительности окна регистрации квантового состояния

Тактико-технические характеристики адаптированного ДОФ

Наименование параметра	Значение	Примечание
Квантовая эффективность регистрации одиночных фотонов, не менее	25 %	отношение количества зарегистрированных фотонов к общему числу фотонов
Частота темновых отсчетов (при значении квантовой эффективности 10%), не более	1000 Гц	количество ложных срабатываний детектора в единицу времени при отсутствие входного оптического сигнала (самосрабатывания)
Время восстановления после срабатывания («мертвое» время детектора)	1..100 мкс	время после срабатывания ДОФ, в течении которого запрещена регистрация поступающих фотонов
Частота стробирования, не менее	100 МГц	количество измерений оптического сигнала в единицу времени
Эффективная ширина строба	0,5..5 нс	длительность временного окна регистрации оптического сигнала

ДОФ на основе однофотонного лавинного фотодиода

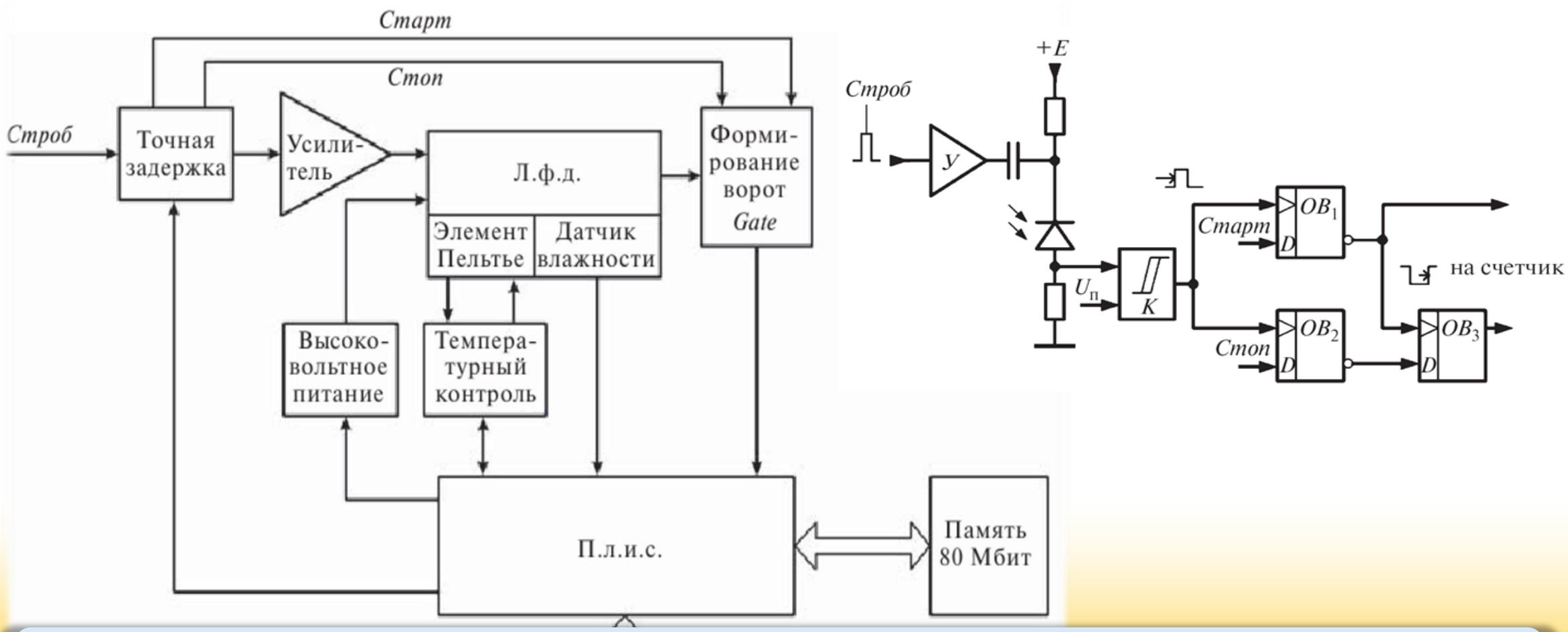




Работа однофотонного лавинного фотодиода (ОЛФД) в Гейгеровском режиме

- используется обратное включение ОЛФД (сила тока пропорциональна интенсивности излучения)
- для регистрации одиночных фотонов напряжение повышается выше напряжения пробоя (Vbr)
- повышенное напряжение подается импульсами во временное окно измерения (стробами)

Структурная схема детектора одиночных фотонов

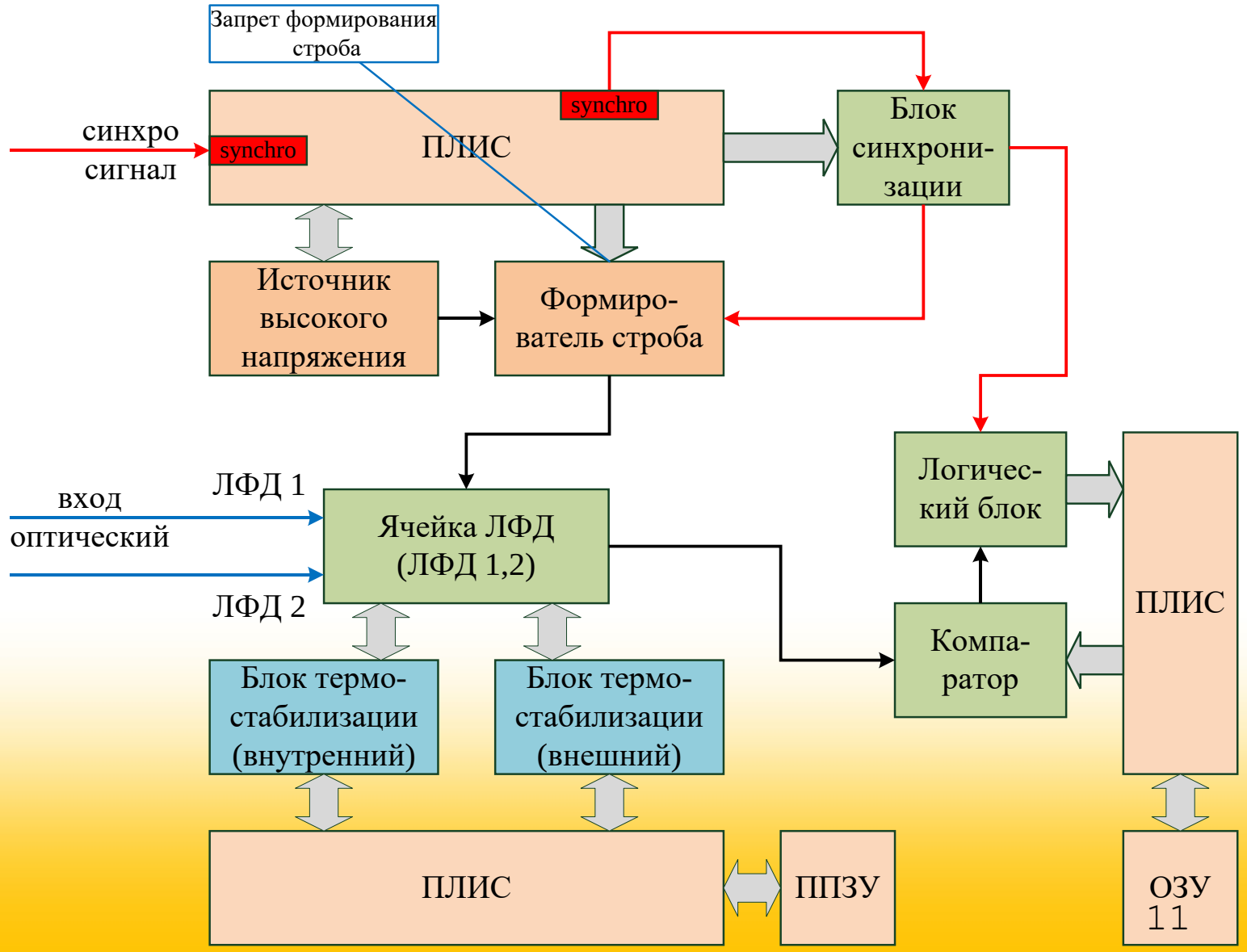


К. А. Балыгин, В. И. Зайцева, А. И. Климова, А. Н. Климов, С. П. Кулик, С. Н. Молотков
Модуль регистратора однофотонных сигналов // Приборы и техника эксперимента, 2018, №4

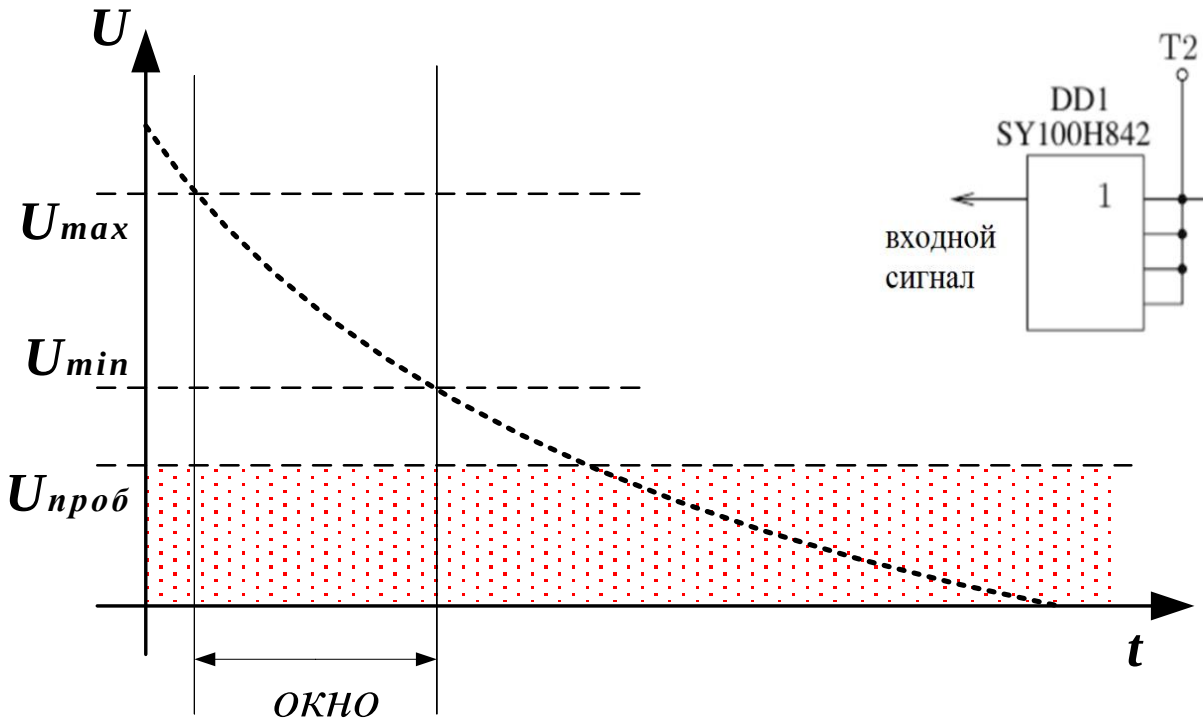
Структурная схема детектора одиночных фотонов

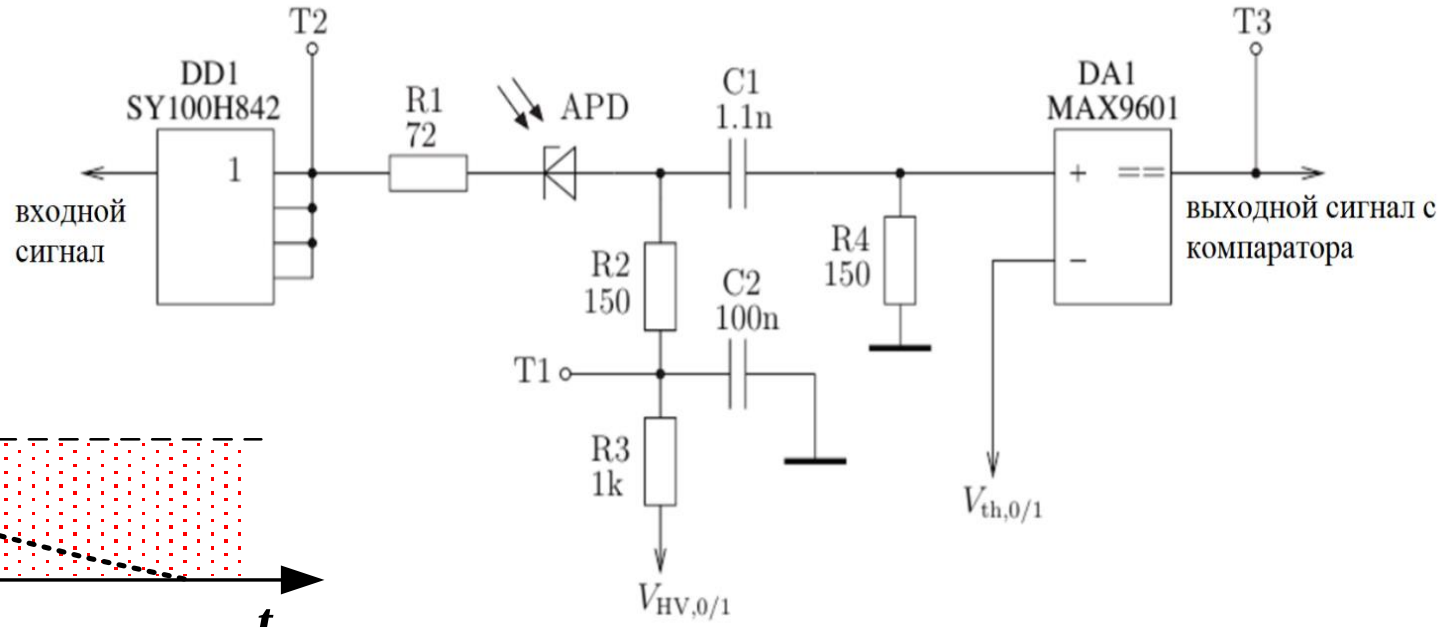
Структурные элементы ДОФ

- модуль ПЛИС с процессорным ядром и ОЗУ
- блок синхронизации
- блок термостабилизации ОЛФД
- источник высокого напряжения
- формирователь стробирующего импульса (строба)
- блок компаратора (оцифровка сигнала ОЛФД)
- логический блок (привязка временного окна измерения и тактовой частоты ПЛИС)



Адаптация ДОФ (*управляемый прямоугольный стробирующий импульс*)



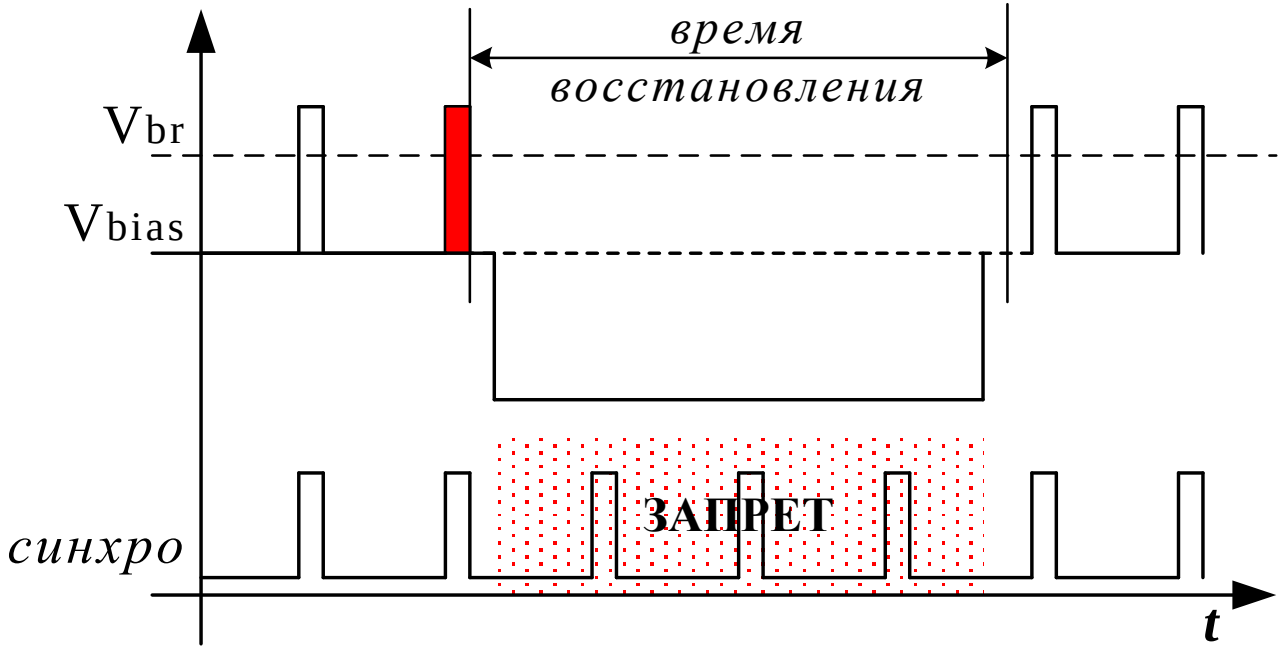


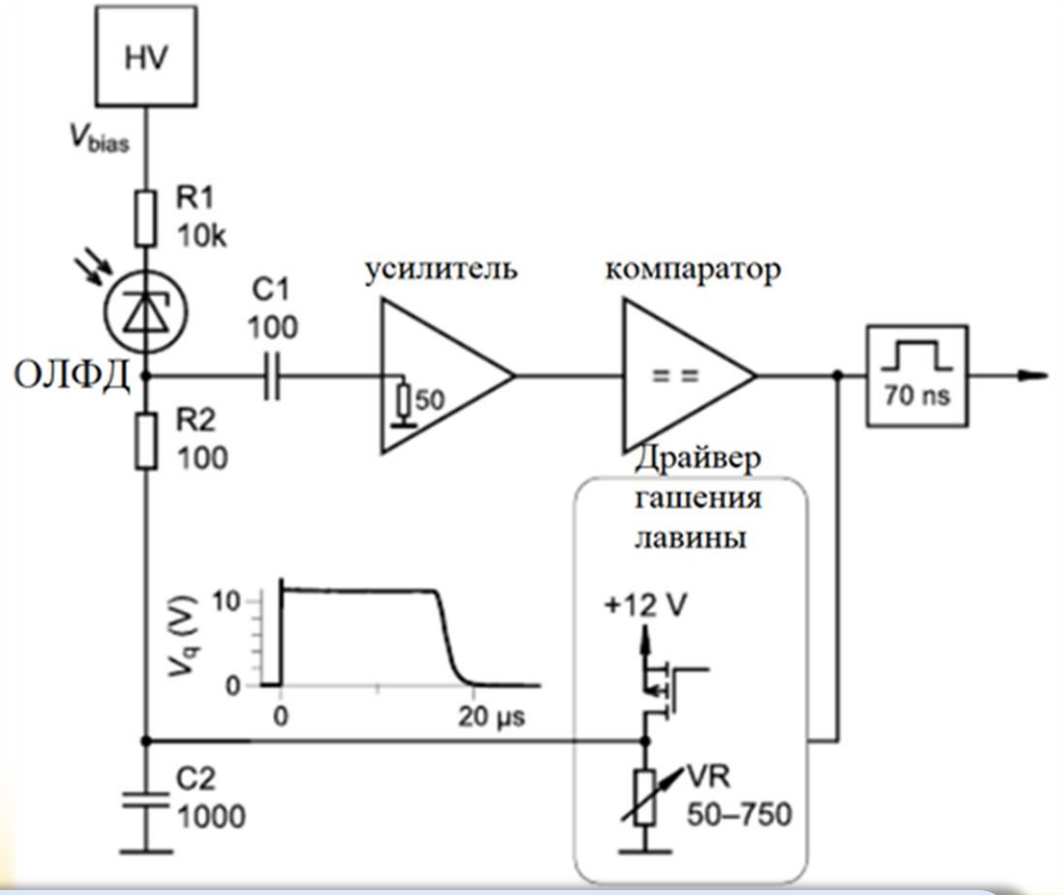
Конденсаторная схема формирования стробирующего импульса

- обратное напряжение ***меняется*** внутри временного окна измерения оптического сигнала
- квантовая эффективность пропорциональна обратному напряжения (***непостоянна***)
- вероятность срабатывания ОЛФД после временного окна измерения (***снижение*** скорости счёта)

➢ реализован переход к схеме с *прямоугольным* стробирующим импульсом *регулируемой длительности*

Адаптация ДОФ (*активное гашение лавины*)





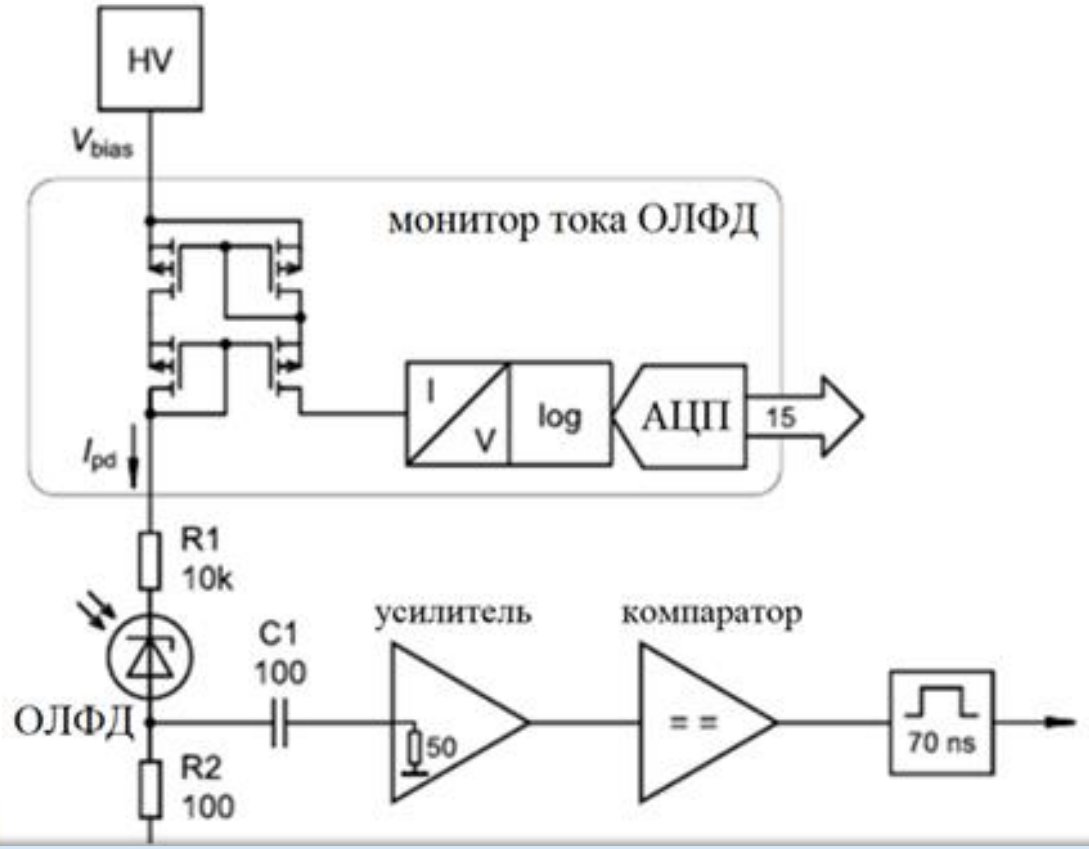
Активное гашение лавины ОЛФД

- уменьшает время восстановления ОЛФД после срабатывания (пробоя)

➢ может реализоваться через снижения напряжения на источнике высокого напряжения

➢ может реализовываться через смещение «земли» ОЛФД к источнику высокого напряжения

Адаптация ДОФ (*защита от неконтролируемой засветки ОЛФД*)



Защита от неконтролируемой засветки ОЛФД

- мощное оптическое излучение приводит к пробою ОЛФД его переводу в линейный режим
- в линейном режиме ток через ОЛФД значительно больше тока ожидания

➢ для защиты от засветки используется мониторинг тока через ОЛФД на основе токового зеркала

Основные выводы

реализован метод совместной передачи классических и квантовых сигналов

- выбран метод совместного использования существующей инфраструктуры ВОЛС для передачи квантовых и классических сигналов в рамках одного оптического волокна при работе аппаратуры КРК с адаптированным детектором одиночных фотонов на основе мультиплексирования оптических сигналов по длине волны
- предложены пассивные методы снижения влияния мощных классических каналов на работу квантового канала аппаратуры КРК на основе оптических фильтров

разработан адаптированный ДОФ для работы аппаратуры КРК на ВОЛС

- определены наиболее критичные структурные элементы ДОФ к совместной передаче квантовых и классических сигналов
- разработаны предложения по доработке структурных элементов ДОФ
- разработан концепт детектора одиночных фотонов, адаптированный под совместную передачу квантовых и классических сигналов в одном оптическом волокне

МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ОТЗЫВ
РУКОВОДИТЕЛЯ МАГИСТЕРСКОЙ ДИССЕРТАЦИИ

Магистерская работа на тему: «Разработка методов и подходов совместной передачи классических оптических импульсов и квантовых состояний»

Выполнена студентом Филиппов Алексей Викторович

Факультет ИТЭ

Кафедра «Нано- и микроэлектроника» Группа 22 ПДм1

Направление подготовки 11.04.04 «Электроника и наноэлектроника», профиль «Нано- и микроэлектроника»

Квалификация (степень) Магистр

Руководитель к.ф.-м.н. Карманов Андрей Андреевич

Качества выпускника, выявленные в ходе выполнения магистерской работы:

В ходе выполнения магистерской диссертации Филиппов А.В. показал отличные навыки работы с оптическими и оптоэлектронными элементами, используемыми в составе систем квантового распределения ключей. Продемонстрированы отличные знания в области квантовой информатики, квантовых вычислений, квантовой и оптической электроники, наноэлектроники, а также информационной безопасности. Разработаны методы и подходы совместной передачи классических оптических импульсов и квантовых состояний в одном оптическом волокне. Предложена структурная схема и схема управления адаптированным детектором одиночных фотонов. Результаты исследовательской работы представлены в патентах РФ на изобретение № 2817659 «Динамическая система формирования и распределения ключей без компрометации ключевой информации» и № 2792414 «Способ передачи информации между конечными узлами связи через промежуточные узлы без перешифрования».

Заключение:

Выполненная выпускником магистерская диссертация полностью соответствуют техническому заданию. Степень соответствия подготовленности выпускника отвечает требованиям к результатам освоения программы магистратуры ФГОС ВО по направлению подготовки 11.04.04 «Электроника и наноэлектроника». На основании вышеизложенного считаю, что магистерская диссертация заслуживает оценки «отлично», а ее автор, Филиппов А.В., присвоения квалификации «магистр» по направлению подготовки 11.04.04 «Электроника и наноэлектроника».

«17» июня 2024 г.

Руководитель Карманов А.А.

РЕЦЕНЗИЯ
на выпускную квалификационную работу
Филиппова Алексея Викторовича

На тему: «Разработка методов и подходов совместной передачи классических оптических импульсов и квантовых состояний»

Целью рецензируемой работы является разработка подходов и методов использования существующей инфраструктуры волоконно-оптических линий связи для совместной передачи классических оптических сигналов телекоммуникационного оборудования и однофотонных квантовых состояний аппаратуры квантового распределения ключей с адаптированным детектором одиночных фотонов. Данная тема исследования является актуальной задачей.

Технология квантового распределения ключей является перспективным направлением в области информационной безопасности автоматизированных информационных систем и критической инфраструктуры. Однако основным сдерживающим фактором, ограничивающим использование аппаратуры квантового распределения ключей, является отсутствие «темных» волокон в существующей инфраструктуре волоконно-оптических линий связи.

Ключевой аспект практической значимости результатов работы заключается в использовании существующей инфраструктуры волоконно-оптических линий связи для организации квантового канала аппаратуры квантового распределения ключей. Достоверность результатов обеспечивается использованием современных методов исследований, в том числе с применением математического моделирования уровня квантовых битовых ошибок при работе аппаратуры квантового распределения ключей.

Рецензируемая работа содержит текстовый материал на 85 страницах с 21 рисунком, библиография – 51 наименование. Работа выполнена в полном соответствии с техническим заданием, на высоком уровне, отражает уверенное владение автором положениями общетехнических и специальных дисциплин, современной техникой исследований.

В работе не показана природа зашумления квантового канала мощным оптическим излучением классических каналов, что можно отнести к её недостаткам, не снижающим научной и практической ценности работы.

В целом считаю, что выпускная квалификационная работа соответствует всем требованиям, предъявляемым к магистерским диссертациям по направлению подготовки 11.04.04 «Электроника и наноэлектроника», заслуживает оценки «отлично», а её автор Филиппов Алексей Викторович, присвоения квалификации магистр по данному направлению обучения.

С.н.с., АО «НИИФИ», к.т.н. Тюрин М.В.

Подпись Тюрина М.В. заверяю
начальник отдела кадров Лопченкова Т.Н.