МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и
радиоэлектроники»

УДК 004.056.5:535.14

На правах рукописи

МАХОРИН ДМИТРИЙ АЛЕКСЕЕВИЧ

МОДЕЛЬ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА С ВРЕМЕННЫМ КОДИРОВАНИЕМ ПО ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ

Специальность 05.11.07 – «Оптические и оптико-электронные приборы и комплексы»

ДИССЕРТАЦИЯ

на соискание учёной степени
кандидата технических наук

Научный руководитель:
доктор физ.-мат. наук, профессор
Задорин Анатолий Семенович

ТОМСК – 2016

ОГЛАВЛЕНИЕ

Сокращения

q-BER - коэффициента квантовых ошибок

tb-кубиты (time-bin qubits) – временные кубиты

АЕ – Агент Е, нелегитимный пользователь

ВК – временное кодирование

ВОЛС - волоконно-оптическая линия связи

ИМЦ – интерферометр Маха-Цендера

КК – квантовый канал

КлК - классический канал

КМ – клон-машина

КРК – квантовое распределение ключа

КС – кодовые состояния

ОВ - оптическое волокно

ПА – Пользователь А, передающая сторона системы КРК

ПБ – Пользователь Б, приемная сторона системы КРК

ПК – поляризационное кодирование

ПОМ – передающий оптический модуль

ПрОМ - приемный оптический модуль

ПрОМ – приемный оптический модуль

ТЗК – теорема о запрете клонирования

ТС – тайм-слот

ВВЕДЕНИЕ

Для организации конфиденциальных каналов передачи данных широкое распространение получили методы шифрования с открытым ключом (асимметричное шифрование), пришедшие на смену симметричному шифрованию, которое обладает существенным недостатком – необходимостью надежного распределения секретного ключа для передающей и приемной стороны.

Защищенность систем с использованием асимметричного шифрования ограничена, как известно, вычислительными возможностями аппаратуры нелегитимного пользователя. В этой связи подобные криптографические алгоритмы принято считать условно защищенными.

Однако перспективы создания принципиально новых вычислительных машин, так называемых квантовых компьютеров, позволит существенно увеличить скорость вычислений, что существенно снизит криптостойкость систем с открытым ключом, поэтому актуальной задачей является поиск альтернативных методов шифрования.

Развитие науки и техники, практическое применение идей квантовой механики в области квантовых вычислений в последние десятилетия позволило разработать системы квантового распределения ключа (КРК), использующие симметричное шифрование. Технология КРК основывается на применении для связи между легитимными пользователями квантовых частиц – фотонов, свойства которых используются для формирования ключевой последовательности $\mathbf{k}_{АБ}$.

Системы КРК обладают существенным преимуществом перед существующими методами шифрования, так как их защищенность от перехвата данных являются безусловной, основанной на физических законах, в том числе на теореме о запрете клонирования (ТЗК) – о невозможности создания точной копии неизвестного квантового состояния, которая была сформулирована Wootters W.K. и Zurek W.H.

Первые протоколы для систем КРК были предложены Bennett C. H. и Brassard G. Практическое и теоретическое развитие данная тема получила в работах Ekert A., Gisin N., Muller. A., Breguet J., Townsend P. и пр. Большой вклад в развитие теории и техники систем КРК внесли отечественные ученые: Молотков С.Н., Кулик С.П., Курочкин В.Л., Неизвестный И.Г., Рябцев И.И., Мазуренко Ю.Т., Кронберг Д.А., Курочкин Ю.В., Голубчиков Д.М., Румянцев К.Е. и др. Исследования в данной области представляют большой интерес в мире.

На данный момент уже созданы коммерческие системы КРК с использованием поляризационного, фазового кодирования, состояний-ловушек (decoy-states). Альтернативным вариантом, отличающимся простотой реализации, а отсюда и относительно низкой стоимостью является временное кодирование квантовых состояний. Данный метод предложен в работах Молоткова С.Н. и Debuisschert T., Boucher W., однако имеет технические сложности в реализации. С целью их преодоления, в том числе с помощью разработки нового метода временного кодирования, было проведено данное диссертационное исследование.

Цель работы: построение программной и аппаратной моделей системы КРК с временным кодированием одно- и двухуровневых однофотонных состояний.

Основные задачи:

1. разработка расчетной и программной моделей оценки помехоустойчивости приемного оптического модуля (ПрОМ) и предельной скорости генерации ключа системы КРК;

2. разработка модели и схемы приготовления многоуровневых временных состояний квантовых частиц для блока кодирования и декодирования системы КРК;

3. разработка структуры и модели подсистем интерферометрического и статистического контроля, а также модели системы КРК с временным кодированием одноуровневых состояний одиночных фотонов с кодированием по протоколу BB84;

4. разработка и исследование метода временного кодирования двухуровневых состояний в системе КРК.

Научная новизна:

1. Показано, что регулировка порога срабатывания решающего устройства в ПрОМ системы КРК по сравнению с существующими цифровыми системами связи позволяет лимитировать вероятность ложных сигналов за счет снижения средней битовой скорости формирования ключа.

2. Показано, что использование статистического и интерферометрического контроля одноуровневых состояний в системах КРК с временным кодированием по сравнению с известными аналогами позволяет усилить защищенность системы.

3. Разработан оригинальный способ построения системы КРК с временным кодированием tb-кубитов, передаваемых по ККС.

4. Предложено использование данных о состоянии кубитов на выходе ККС не прошедших процедуру согласования базисов в рамках протокола BB84 для детектирования перехвата данных

5. Предложен оригинальный способ обнаружения атак на систему КРК, заключающийся в обработке временного статистического распределения сигналов на выходе ПрОМ по тайм-слотам (минимальным временным интервалам, в пределах которых может быть детектирован фотон, ТС) в пределах тактового интервала.

Практическая значимость:

1. Предложена модель оценки помехоустойчивости ПрОМ с ЛФД, работающем в линейном режиме. Установлена зависимость уровней вероятности ложного сигнала P_f и пропуска сигнала P_l, а также средней битовой скорости генерации ключа от вариации порога срабатывания решающего устройства.

2. Предложена и исследована схема контроллера ЛФД ПрОМ для высоковольтных диодов в линейном и гейгеровском режиме с активным

гашением лавины в виде формирователя импульсов перенапряжения с разрядной линией.

3. Разработаны и исследованы модели подсистем интерферометрического и статистического контроля, а также модель системы КРК с временным кодированием одноуровневых состояний одиночных фотонов по протоколу BB84.

4. Предложена модель описания способа приготовления tb-кубитов в системе из нескольких разбалансированных интерферометров Маха-Цендера (ИМЦ).

5. Предложена модель описания способа приготовления tb-кубитов в системе из нескольких разбалансированных интерферометров Маха-Цендера (ИМЦ).

6. Предложено использование дополнительного оптического волокна, соединяющего свободные порты ИМЦ-А, Б при контроле интерференции амплитуд вероятности КЧ в квантовом канале, позволяющего увеличить системный битрейт в два раза по сравнению с аналогичными оптоволоконными системами КРК с фазовым кодированием.

Положения, выносимые на защиту:

1. Использование в ПрОМ ЛФД S8664-05K, в линейном режиме при комнатной температуре, может обеспечить среднюю битовую скорость генерации ключа системой КРК 10,2 Кб/с при вероятности ошибок P_f =0,07.

2. Применение tb-кубитов позволяет реализовать протокол BB84 в формате временного кодирования.

3. В системах КРК с временным кодированием tb-кубитов детектирование работы клон-машины нелегитимного пользователя может обеспечиваться за счет контроля распределения вероятностей регистрируемых квантовых частиц по тайм-слотам тактового интервала.

4. Контроль динамических состояний всех поступивших из квантового канала системы КРК с временным кодированием tb-кубитов позволяет более чем в два раза повысить объем информации, используемой для детектирования присутствия в системе нелегитимного пользователя.

Достоверность полученных результатов диссертационного исследования обеспечивается обоснованностью предлагаемых моделей, решений и выводов, верификацией полученных результатов с имеющимися теоретическими и экспериментальными данными, результатами симуляции на ЭВМ.

Личный вклад автора.

Все представленные в диссертации результаты исследований получены лично автором либо при его непосредственном участии.

Обоснование структуры работы.

Диссертация состоит из введения; четырех глав; заключения, списка литературы и 4 приложений. Общий объем диссертации – 132 страницы, в том числе рисунков и схем – 63. Список использованной информации содержит 111 наименований.

Публикации и апробация работы.

Основные положения работы докладывались и обсуждались на следующих конференциях, семинарах, выставках:

1. XVII Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых «Научная сессия ТУСУР – 2012», г. Томск, 16-18 мая 2012г.
2. VIII Международная научно-практическая конференция «Электронные средства и системы управления - 2012», г. Томск, 8-10 ноября 2012г.
3. V Международная научно-практическая конференция «Актуальные проблемы радиофизики - 2013», г. Томск., 1-6 октября 2013г.
4. IX Международная научно-практическая конференция «Электронные средства и системы управления - 2013», г. Томск, 30-31 октября 2013г.
5. X Международная научно-практическая конференция «Электронные средства и системы управления - 2014», г. Томск, 12-14 ноября 2014г.
6. 25-ая Международная Крымская конференция «СВЧ-техника и телекоммуникационные технологии», г. Севастополь, 6-12 сентября 2015г.
7. XI Международная научно-практическая конференция «Электронные средства и системы управления - 2014», г. Томск, 25-27 ноября 2015г.

По результатам исследований опубликованы 13 печатных работ, из которых в рекомендованных ВАК РФ периодических изданиях – 8. Было получено свидетельство о государственной регистрации программы для ЭВМ (Приложение А).

Работы, опубликованные автором в ведущих рецензируемых научных журналах, рекомендованных ВАК Министерства Образования и Науки Российской Федерации:

1. Задорин А.С., Максимов А.В., Махорин Д.А. и др. Скорость генерации кода в системе квантового распределения ключей // Доклады ТУСУРа. – 2011. – № 2 (24). – С. 139-141

2. Задорин А.С., Максимов А.В., Махорин Д.А. Режимы работы фотоприемного устройства системы квантовой криптографии // Доклады ТУСУРа. – 2012. - №2(26). – С. 63-66

3. Махорин Д.А., Галиев А.Б., Задорин А.С. Возможность реализации линейного режима счета фотонов на лавинном фотодиоде S8664-05K при комнатной температуре // Доклады ТУСУРа. – 2013. – №1(31). – С. 65-68

4. Задорин А.С., Махорин Д.А. Модель системы квантового распределения ключей с временным кодированием // Доклады ТУСУРа. – 2014. – №3 (33). – С. 85-89.

5. Задорин А.С., Махорин Д.А. Статистическая обработка сигналов в системах квантового распределения ключей // Доклады ТУСУРа. – 2014. – №3 (33). – С. 90-93.

6. Задорин А.С., Махорин Д.А. Интерферометрический контроль целостности данных в системе квантового распределения ключей с временным кодированием // Доклады ТУСУРа. – 2014. – №4 (33). – С. 85-89.

7. Задорин А.С., Махорин Д.А. Матричное описание трансформации квантовых состояний одиночных фотонов в последовательности разбалансированных интерферометров Маха-Цендера // Доклады ТУСУРа. – 2015. – №3 (37). – С. 145-149.

8. Задорин А.С., Махорин Д.А. Принцип квантового распределения ключей по оптическому волокну на основе временных сдвигов tb-кубитов // Изв. вузов. Физика. – 2016. – Т.69, № 3. – с. 24-29.

Другие работы, опубликованные автором по теме диссертации:

9. Махорин Д.А. Особенности гейгеровского режима работы фотоприемного устройства системы КРК // Материалы докладов XVII Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР – 2012», г. Томск, 16-18 мая 2012г.

10. Авдоченко Б.И., Задорин А.С., Максимов А.В., Махорин Д.А. Контроллер лавинного фотодиода системы квантовой криптографии // Материалы докладов VIII Международной научно-практической конференции «Электронные средства и системы управления - 2012» – Томск, 8-10 ноября 2012г. часть 2. – С. 105-109.

11. Махорин Д. А., Задорин А. С., Альбрехт Р. С., Исатаев А. Н. Усиление защищенности системы квантового распределения ключа с временным кодированием по оптическому волокну // Международная конференция «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2015), материалы 25-й международ. конф. – Севастополь, 2015. том 1 – С. 1019-1021.

12. Задорин А.С., Махорин Д.А. Временное кодирование состояний фотонов в системе квантового распределения ключей с временным кодированием tb-кубитов // Материалы докладов XI Международной научно-практической конференции «Электронные средства и системы управления - 2014», г. Томск, 25-27 ноября 2015г. Часть. 1. С. 265-269.

13. Махорин Д.А., Задорин А.С., Решетников С.Ю. Статистический контроль распределения числа фотонов в информационных сообщениях в системе квантового распределения ключа с временным кодированием // Материалы докладов XI Международной научно-практической конференции «Электронные средства и системы управления - 2014», г. Томск, 25-27 ноября 2015г. Часть. 1. С. 270-273.

14. Свид. о государственной регистрации программы для ЭВМ №2015617171. Махорин Д.А., Задорин А.С. Quantum key distribution system. Зарег. в Реестре программ для ЭВМ 2 июля 2015 г.

1. ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА

В данной главе рассматриваются некоторые особенности поведения одиночных квантовых объектов, а также общие принципы построения системы КРК: протоколы, способы кодирования, а также элементную базу, используемую для построения таких систем.

1.1 Принципы квантовой механики

При описании работы систем квантового распределения ключа в дальнейшем воспользуемся следующими принципами квантовой механики:

1. Принцип суперпозиции состояний. Любая микросистема, такая как атом, молекула или частица, в данном состоянии может рассматриваться как находящаяся частично в каждом из двух или более других состояний, т.е. любое состояние может рассматриваться как суперпозиция. Их можно реализоваться бесконечным числом разных способов [1, 2].

2. Принцип недетерминированности. Наблюдение, производимое над микросистемой, заставляет ее принять одно или более конкретное состояние (что связано с типом измерения). Невозможно предсказать, в какое именно состояние перейдет данная система, но можно предсказать вероятность перехода конкретной системы в данное конечное состояние [2].

3. Бритва Дирака. Квантовая механика отвечает только на вопросы, связанные с результатами возможных экспериментов, а любые другие вопросы лежат вне ее сферы [1].

1.1.1 Описание состояния квантовой частицы

В общем случае вектор состояния квантовых частиц $|\psi\rangle$ [3, 4] представляет собой многомерный объект гильбертова пространства [5, 6], однако во многих системах КРК [7, 8] состояние $|\psi\rangle$ приготавливается в двумерном ортогональном базисе некоторой наблюдаемой, связанной с соответствующим эрмитовым оператором измерения **A** [9, 10],

$$|\psi_2\rangle=\alpha|0\rangle+\beta|1\rangle, \qquad (1.1)$$

где $|0\rangle$, $|1\rangle$ и α, β – соответственно, собственные векторы-столбцы оператора **A** и амплитуды вероятности нахождения частицы в данных состояниях, которые в общем случае являются комплексными числами. Индексом 2 здесь отмечено число возможных состояний частицы. Вектор-столбец называется «кет-вектор» [2, 10, 11, 12].

Соотношение (1.1) устанавливает вид кодирования квантовой частицы в системе КРК, т.е. связь информационной составляющей с ее физическим свойством, и представляет собой элементарный квантовой бит - кубит [8, 13, 14]. В качестве его физической реализации может быть фотон или электрон. Векторы $|0\rangle$, $|1\rangle$ составляют вычислительный базис кубита [7, 14, 15].

До измерения кубит имеет оба логических значения, т.е. находится в обоих состояниях вычислительного базиса одновременно, а измерение позволяет кубиту коллапсировать в одно из этих состояний. Это отличается от классического подхода, в рамках которого предполагается, что бит до измерения находится в одном из логических состояний, а измерение только обнаруживает этот факт.

Состояние вычислительного базиса являются ортогональными, поэтому с практической точки зрения векторами вычислительного базиса являются состояния фотона с горизонтальной или вертикальной поляризацией, или состояние электрона, характеризуемые направлением спина вверх или вниз [13].

Важно отметить, что отличие когерентной суперпозиции [1, 17] от некогерентной смеси [2, 14, 18] состоит в том, что для первой всегда существует базис, в котором возможные значения кубита строго определены [15]. При этом когерентное состояние есть состояние, в котором величины неопределенностей амплитуды и фазы равны [19].

Условие нормировки имеет вид:

$$\langle\psi|\psi\rangle=|\alpha|^2+|\beta|^2=1. \qquad (1.2)$$

где $\langle\psi|$ - бра-вектор [1].

Таким образом, состояние кубита можно рассматривать как вектор в двумерном комплексном векторном пространстве. Условие (1.2) тогда означает, что этот вектор имеет единичную длину [2, 14].

1.1.2 Интерференция амплитуд вероятности состояния квантовой частицы

Рассмотрим известный опыт Юнга [16, 20] по интерференции света с использованием двух щелей (рис. 1.1). Распределение интенсивности падающего света описывается кривой I_x и имеет интерференционный характер.

Если уменьшать интенсивность света, характер данной кривой не будет изменяться даже в том случае, если источник будет испускать единичные фотоны. Аналогичная ситуация наблюдается и при использовании источника моноэнергетических электронов. Таким образом, явление интерференции объясняется свойствами отдельного объекта, а не их коллективов [20].

Попытки отследить через какую именно щель прошел фотон приводят, также как и при закрытии одной из щелей, к изменению картины на экране-детекторе – интерференция пропадает.

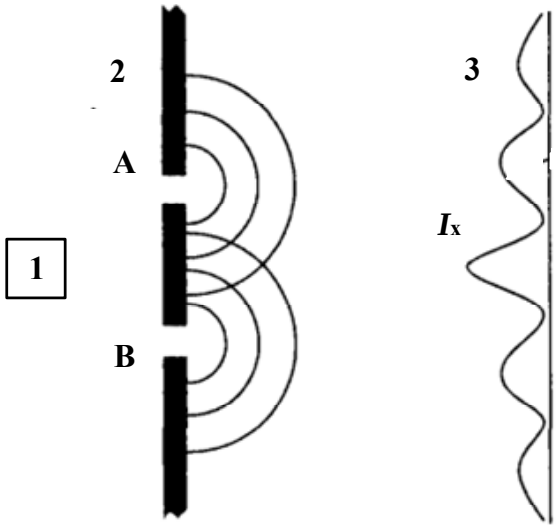


Рис. 1.1. Опыт Юнга по интерференции света с использованием двух щелей, где 1 – источник монохроматического света, 2 – пластина со щелями А и Б, 3 – экран-детектор.

Для описания данных эффектов в квантовой физике используется амплитуда вероятности некоторого *s*-состояния квантовой частицы. С ее помощью переход частицы из начального *s*-состояния в конечное *f*-состояние (регистрация вблизи координаты *x* на экране-детекторе) определяется квадратом модуля скалярного произведения $\langle f|s\rangle$:

$$\omega_{s\to f} = |\langle f|s\rangle|^2$$

Частица при этом проходит через щели *А* или *Б*, т.е. есть две альтернативы. Амплитуды вероятностей для этих альтернатив записываются как:

$$\langle x \mid s\rangle_A = \langle x \mid A\rangle \langle A \mid s\rangle,$$

$$\langle x \mid s\rangle_Б = \langle x \mid Б\rangle \langle Б \mid s\rangle.$$

Когда обе щели открыты, данные альтернативы в таких условиях опыта неразличимы. По этой причине результирующая вероятность перехода $s\to x$ имеет вид:

$$|\langle x \mid s\rangle|^2 = |\langle x \mid s\rangle_A + \langle x \mid s\rangle_A|^2 = |\langle x \mid s\rangle_A|^2 + |\langle x \mid s\rangle_Б|^2 +$$

$$+ \langle x \mid s\rangle_A \langle x \mid s\rangle_Б^* + \langle x \mid s\rangle_A^* \langle x \mid s\rangle_Б .$$

Кривая *I*(x), которая регистрируется на экране-детекторе, соответствует распределению попаданий частиц, что определяется вероятностью $|\langle x|s\rangle|^2$. Интерференционный характер *I*(x) объясняется наличием в $|\langle x \mid s\rangle|^2$ слагаемых $\langle x \mid s\rangle_A \langle x \mid s\rangle_Б^*$ и $\langle x \mid s\rangle_A^* \langle x \mid s\rangle_Б$. В результате интерференционное распределение попаданий фотонов или электронов на экране-детекторе, в том случае если обе щели открыты, является следствием интерференции амплитуд вероятности перехода частицы из заданного начального в заданное конечное состояние [20].

1.1.3 Теорема о запрете клонирования состояний квантовых частиц

Защищенность кодирования состояния одиночной квантовой частицы в системе КРК основывается на теореме о запрете клонирования [13, 21, 22], которая гласит, что невозможно создать точную копию неизвестного квантового состояния.

Рассмотрим доказательство ТЗК более подробно. Предположим, что существует преобразование Q, реализующее функцию копирования произвольной квантовой суперпозиции $|\psi\rangle$, при этом отметим, что данное преобразование не обязательно должно быть унитарным. Единственным условием будет то, что Q можно расширить до унитарного оператора U, действующего на замкнутую систему, состоящую из подсистемы в состоянии $|\psi\rangle$, которую нужно клонировать, и соответствующего окружения $|\Omega\rangle$. Состояние $|0\rangle$ на ее входе необходимо для того, чтобы уравнять число входов и выходов, что является важным для унитарных матриц.

Если бы было возможно реализовать такой оператор U, то имелась бы вероятность построения клонирующего устройства Q, поэтому необходимо проверить существование оператора U. Наиболее подходящей проверкой унитарности является то, что унитарные операторы сохраняют внутреннее произведение. Используем две произвольные суперпозиции $|\psi_{S1}\rangle$ и $|\psi_{S2}\rangle$, копирование каждой из них будет выглядеть следующим образом:

$$U : |\psi_{S1}\rangle|0\rangle|\Omega\rangle \rightarrow |\psi_{S1}\rangle|\psi_{S1}\rangle|\Omega_1\rangle,$$

$$U : |\psi_{S2}\rangle|0\rangle|\Omega\rangle \rightarrow |\psi_{S2}\rangle|\psi_{S2}\rangle|\Omega_2\rangle,$$

где $|\Omega_1\rangle$ и $|\Omega_2\rangle$ описывают состояния окружения после успешного клонирования соответствующих суперпозиций. Тогда внутреннее произведение состояний на входе будет:

$$\langle\Omega, 0, \psi_{S2} \mid \psi_{S1}, 0, \Omega\rangle = \langle\psi_{S2} \mid \psi_{S1}\rangle \langle 0|0\rangle\langle\Omega \mid \Omega\rangle = \langle\psi_{S2} \mid \psi_{S1}\rangle,$$

тогда на выходе получается

$$\langle\Omega_2, \psi_{S2}, \psi_{S2} \mid \psi_{S1}, \psi_{S1}, \Omega_1\rangle = \langle\psi_{S2} \mid \psi_{S1}\rangle\langle \psi_{S2} \mid \psi_{S1}\rangle\langle\Omega_2 \mid \Omega_1\rangle = \langle\psi_{S2} \mid \psi_{S1}\rangle^2\langle\Omega_2 \mid \Omega_1\rangle.$$

Правые части будут равны в том случае если $\langle\psi_{S2}|\psi_{S1}\rangle = \pm 1$, что равносильно $|\psi_{S1}\rangle=|\psi_{S2}\rangle$ либо в случае $\langle\psi_{S2}|\psi_{S1}\rangle = 0$, что равносильно ортогональности $|\psi_{S1}\rangle$ и $|\psi_{S2}\rangle$. Других возможностей обеспечить внутреннее произведение с условием того, что оно будет равно или меньше 1, не существует.

В результат, ТЗК утверждает то, что копирование возможно только для ортогональных квантовых состояний [13]. Именно данный факт используется при построении систем КРК.

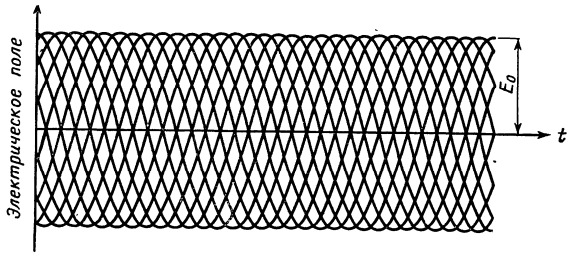
1.2 Приготовление состояний квантовых частиц

Для вектора $|\psi\rangle$ известное соотношение неопределённостей энергия-время может быть выражено через неопределенность фазы $\Delta\phi$ и числа фотонов Δn [23]:

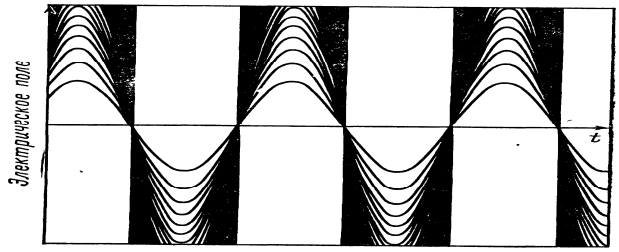
$$\delta t \cdot \delta E = \frac{\delta\phi}{\omega} \geq \frac{\hbar}{2} \Leftrightarrow \delta\phi \cdot \delta n \geq \frac{1}{2}. \qquad (1.3)$$

Из (1.3) следует, что предел точности определения фазы $\Delta\phi$ амплитуды вероятности вектора состояния $|\psi\rangle$ ограничен точностью Δn.

В качестве иллюстрации на рис. 1.2 приведены взятые из [24] динамические зависимости квантовых полей приготовленных для Δn=0 и $\Delta\phi$=0 соответственно.



а. Графическое описание изменения электрического поля со временем в фиксированной точке при Δn=0



*б.*Графическое описание изменения электрического поля со временем в фиксированной точке при $\Delta\phi$= 0

Рис. 1.2. Зависимости квантовых полей при фиксированном значении числа фотонов и фазы

Квантовые состояния с точно определенным числом фотонов (Δn=0), соответствующие рис. 1.2 (а), называются состояниями Фока, или фоковскими состояниями [19], а состояния с наименьшими неопределенностями фазы и числа фотонов, когда $\delta\phi \cdot \delta n = \frac{1}{2}$ – когерентными состояниями [19].

На практике используются различные способы приготовления вектора состояния $|\psi\rangle$. Одним из основных параметров, характеризующих статистические свойства состояния $|\psi\rangle$ является статистический параметр Манделя ξ, связанный с дисперсией числа квантов Δn^2 следующим образом [19]:

$$(\triangle n^2) = \langle \hat{n} \rangle (1 + \xi). \tag{1.4}$$

Если ξ,=0, то вектор $|\psi\rangle$ находится в когерентном состоянии, наиболее близком к классическому, при ξ,>0 - в суперпуассоновском состоянии, которое также является классическим, а при ξ,<0 в неклассическом субпуассоновском состоянии.

Рассмотрим подробнее особенности приготовления $|\psi\rangle$, а также соответствующие значения параметр Манделя ξ.

1.2.1 Приготовление фоковских состояний

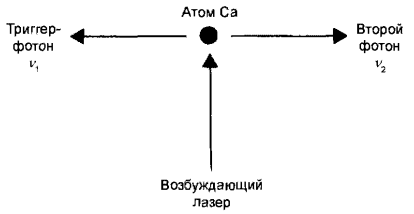
Состояния Фока $|n\rangle$ являются собственными состояниями оператора числа фотонов **n** [19, 24]:

$$\hat{n}|n\rangle = n|n\rangle.$$

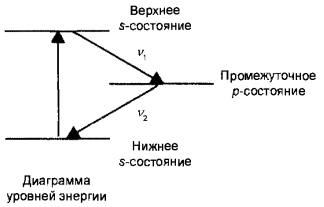
Вектор $|\psi\rangle$ в состояниях Фока $|n\rangle$ характеризуются в состоянии с точным числом фотонов (Δn=0), поэтому, в данном состоянии флуктуации числа квантов должны отсутствовать, а статистический параметр Манделя ξ=-1. Состояния Фока сложны для приготовления.

В качестве примера на рис. 1.3 приведена взятая из [25] структурная схема реализации способа приготовления однофотонного фоковского состояния. Здесь источником одиночных фотонов служит атом калия, который под действием лазера переходил в возбужденное состояние. При релаксации он переходит сначала на промежуточный уровень, излучая первый фотон, а затем на основной уровень с испусканием второго фотона, который и используется в эксперименте. При этом первый фотон является триггер-сигналом для фиксации второго фотона.

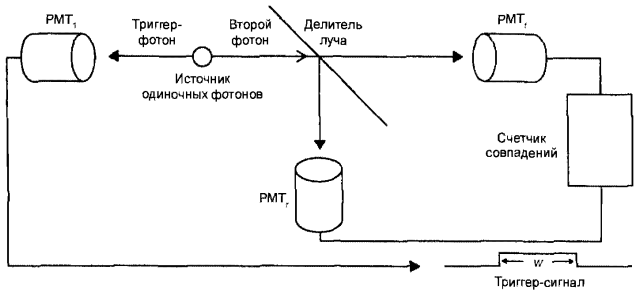
Указанные способы приготовления фоковских состояний одиночных фотонов хотя и идеально соответствуют требованиям протоколов КРК, однако весьма сложны в практической реализации.



а. Возбуждение атома калия



б. Поведение при релаксации



в. Структурная схема установки

Рис. 1.3. Эксперимент по приготовление однофотонного фоковского состояния

1.2.2 Приготовление когерентных состояний

Когерентные состояния $|\alpha\rangle$ являются классическими состояниями светового поля традиционных источников (статистический параметр Манделя $\xi \geq 0$) [19, 24]. В чистом виде такие состояния являются наиболее близким квантово-механическим аналогом свободного классического одномодового поля, например, лазерного источника [24, 25].

Формально когерентные состояния $|\alpha\rangle$ рассматриваются как собственные состояния оператора уничтожения **a**:

$$\hat{\alpha}|\alpha\rangle = \alpha|\alpha\rangle. \tag{1.5}$$

В качестве собственных состояний оператора **a** когерентные состояния обладают точно определенными амплитудами |**a**| и фазами arg(**a**). Поскольку оператор **a** не является эрмитовым, то его собственные значения комплексны. Они соответствуют комплексным амплитудам волны в классической оптике [26].

В фоковском базисе когерентные состояния представляются в виде [19, 24]:

$$|\alpha\rangle = \sum_m e^{-(|a|^2/2)} \frac{a^n}{\sqrt{n!}} |n\rangle. \tag{1.6}$$

Вероятностная интерпретация амплитуды вероятности вектора $|\alpha\rangle$ позволяет установить, что вероятность нахождения n фотонов в когерентном состоянии $|\alpha\rangle$ описывается пуассоновской статистикой:

$$p(n) = e^{-\langle n\rangle} \frac{\langle n\rangle^m}{m!}, \tag{1.7}$$

где $\langle n\rangle = |a|^2$, а соответствующий параметр Манделя $\xi=0$.

Статистические смеси когерентных состояний описывают световые поля теплового происхождения, которые характеризуются суперпуассоновской ($\xi>0$), т.е. отличной от (1.7) статистикой [24].

1.3 Приготовление временных кубитов в интерферометре Маха-Цендера

Перспективы практической реализации теоретических разработок в области оптических квантовых вычислений и систем квантовой передачи информации во многом определяются уровнем развития элементной базы квантовой оптики, а также соответствующих математических и расчетных моделей квантовых вентилей [10, 13, 27, 28]. Специфика квантовых эффектов ограничивает возможности моделирования и оптимизации указанных устройств с помощью существующих оптических CAD-систем, область применения которых

лимитируется рамками традиционной волновой оптики. В данных условиях важной задачей становится разработка адекватных моделей квантовых вентилей [13, 14] (квантовых гейтов – quantum gate [2]), т.е. набора логических квантовых устройств, изменяющих состояния кубита $|\psi\rangle$ в регистре квантового устройства в соответствии с заданным квантовым алгоритмом.

Одним из распространенных однокубитовых квантовых вентилей вычислительных и коммуникационных квантовых схем является интерферометр Маха–Цендера (ИМЦ) [28, 29, 30], предназначенный для приготовления и измерения фазовых сдвигов между амплитудами вероятности в заданном вычислительном базисе кубита [10, 13]. В ИМЦ на аппаратном уровне объединено несколько логических устройств: однокубитовые квантовые вентили Адамара H, представленные волоконными сплиттерами и фазовращающий вентиль, реализованный в виде волоконно-оптического регулятора фазы α в плечах интерферометра P [13], рис. 1.4.

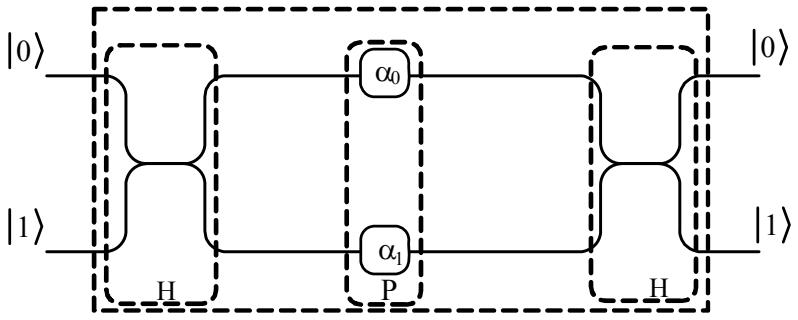


Рис. 1.4. Структурная схема интерферометра Маха-Цендера

Модификация указанного вентиля используется также и для формирования на выходе ИМЦ суперпозиции из двух сдвинутых во времени состояний $|\alpha\rangle$, $|\beta\rangle$, образующих новый динамический измерительный базис кубита $|\psi\rangle$. В литературе такая суперпозиция называется time-bin qubit [31], ниже оно обозначается как временной или tb-кубит. В соответствии с изложенным выше, приготовление такого tb-кубита сопряжено с разбалансировкой интерферометра, а именно, с введением дополнительного отрезка оптического волокна (ОВ) в одно из плеч

ИМЦ и соответствующей задержкой одиночного фотона на время Δ. Интерферометр такого типа широко используется при решении многих задач квантовой оптики [7, 10, 13], однако для его моделирования используются, в основном, дескриптивные подходы, плохо сочетающиеся с традиционным математическим формализмом описания квантовых систем.

Имеется необходимость в обобщении известной модели симметричного ИМЦ [13] на случай одиночного разбалансированного интерферометра, а также системы из нескольких последовательно соединенных ИМЦ.

1.3.1 Интерференция одиночных фотонов в интерферометре Маха-Цендера

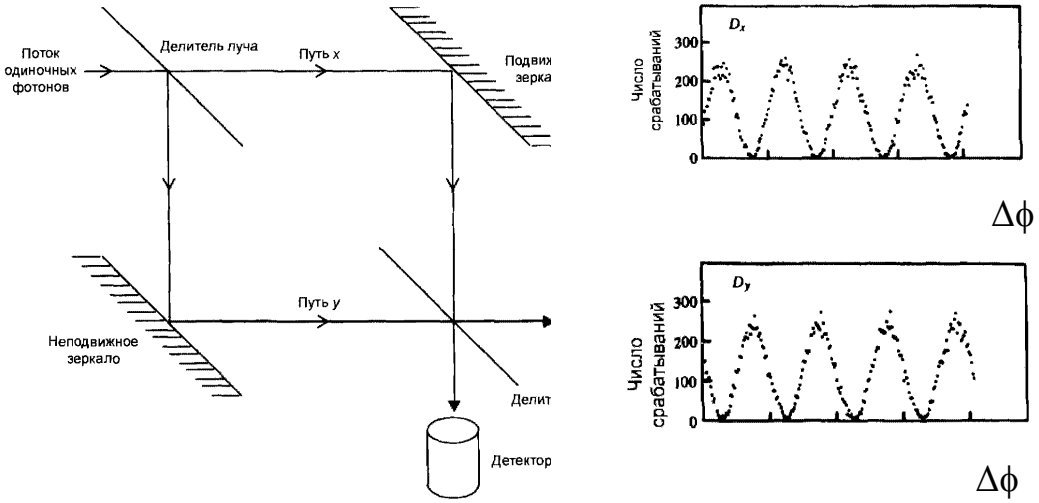
Как отмечалось выше, модуль амплитуды вероятности состояния квантовой частицы однозначно определяет вероятность ее регистрации. Фаза амплитуды вероятности arg(|ψ⟩) также является важной информацией о векторе |ψ⟩, определяется схемой его приготовления и измерения и, в частности, характеризует нелокальный характер состояния |ψ⟩ [25].

В качестве примера обнаружения такой зависимости на рис. 1.5 показана схема и результаты эксперимента группы А. Аспекта по интерференции одиночных фотонов, в интерферометре Маха–Цендера (ИМЦ) [25]. В данном эксперименте состояния вектора |ψ⟩ приготавливалось по схеме рис. 2, так, что оно совпадало с состоянием Фока |*n*⟩. Представленные на рис. 1.5 *б* данные показывают, что рассматриваемые здесь квантовые частицы проявляют нелокальные свойства, позволяющие им проходить по обоим плечам интерферометра одновременно.

Указанное свойство одиночных фотонов образовывать интерференционную картину в выходных портах ИМЦ является физической основой для фазового кодирования квантовых частиц при КРК.

Еще один важный практический вывод, вытекающий из данных рис. 1.5, касается способа приготовления одиночных квантовых частиц. Как отмечалось, в описанном выше эксперименте состояния интерферирующих одиночных фотонов

были фоковскими. Из (1.3) следует, что абсолютная фаза вектора $|n\rangle$ в этом случае (Δn=0) становится полностью неопределенной. Однако, как видно из рисунка 1.5 *б*, сдвиг интерференционной картины определяется относительной фазой состояния $|n\rangle$, а именно, в полном соответствии с концепцией П. А. М. Дирака [1], интерференцией отдельных фотонов самих с собой. Отсюда следует, что картина, аналогичная рис. 1.5 *б*, будет формироваться также и для когерентных состояний (3), как для чистых состояний Глаубера $|\alpha\rangle$, так и для всех возможных их смесей, включая хаотический свет. Отличительной особенностью интерференционной картины в этих случаях будет ненулевой разброс числа фотонов Δn.



а. Схема эксперимента

б. Число срабатываний детекторов в зависимости от разности фаз в плечах ИМЦ.

Рис. 1.5. Эксперимент по интерференции одиночных фотонов в ИМЦ [4,12]

1.4 Протоколы кодирования в системах КРК

Основными протоколами кодирования одиночных состояний фотонов в систем КРК являются протокол BB84, предложенный Беннеттом и Брассардом в 1984 году [32] и B92, разработанный Беннеттом в 1992 году [33]. А также множество

других - BB84 (4+2) [7, 34], с шестью состояниями [35], Гольденберга-Вайдмана [36], Коаши-Имото [37] и проч.

Помимо этого, существуют протокол Экерта, основанный на принципах парадокса Эйнштейна-Подольского-Розенберга, происходит кодирование перепутанных состояний - E91 [38].

Первая экспериментальная демонстрация установки КРК была проведена в 1989 году и осуществлялась на расстояние около тридцати сантиметров через открытое пространство [39]. Далее были эксперименты Мюллера в Женеве с передачей ключа по оптическому волокну длиной 1,1 км [40, 41], в 1995 оно было увеличено до 23 км [42, 43]. Примерно в это же время Таунсендом из British Telecom была показана передача на 30 км [44]. Дальнейшие исследования с различными конфигурациями оптических сетей [45, 46] позволило увеличить дальность до 50км [47]. Эксперименты по передаче данных на это же расстояние были повторены Хьюзом и др. в Лос-Аламосе [48]. В 2001 году Хискетом и др. была проведена передача на расстояние 80 км [49]. В 2004-2005гг. две группы из Японии и одна из Соединенного Королевства рапортовали об удачных экспериментах по квантовому распределению ключей и интерференции одиночных фотонов на расстоянии более 100км [50, 51, 52]. Первые эксперименты по передаче на расстояние свыше 120км проводились учеными из Toshiba в Кембридже [51]. В 2006 году рекорд по дальности передачи данных был побит учеными Лос-Аламоса и Национального института стандартов и технологий и составил 184 км по оптическому волокну [53]. В нем использовались однофотонные приемники, охлажденные до температур близких к нулю по Кельвину [54]. Для открытого пространства в 2006 рекордом стала дальность в 144 км с использованием схемы Экерта [55], а в 2007 с использованием BB84, усиленного с помощью состояний-ловушек [56]

Продемонстрированная в 2008 система, выполненная сотрудниками Toshiba и Кембриджа имела скорость порядка 1 Мб/с при передаче по оптическому волокну на 20км и 10 кбит/с при передаче на более чем 100км [57, 58]. Коммерческая

система от фирмы Toshiba на данный момент обладает возможность передачи на расстояние около 50 км со скоростью 1 Мб/с [59]. В 2014 году была достигнута наибольшая длина квантового канала в 307 км с битрейтом в 12,7 кбит/с [60].

На данный момент создана Группа Отраслевой Спецификации (ISG) Европейского института телекоммуникационных стандартов (ETSI) для решения вопросов стандартизации квантового распределения ключей [61], разрабатываются измерения для характеристики оптических компонентов слабых импульсов систем КРК [62].

Нынешние системы КРК имеют возможность передачи на расстояние более 100 км со скоростями, достаточными для передачи ключей шифрования, но не для поточного шифрования магистральных каналов. В данный момент высокая цена таких систем ограничивает их массовое применение для организации конфеденциальной связи между небольшими и средними фирмами и частными лицами [54], поэтому существует необходимость в разработке простой, т.е. недорогой и надежной системы КРК.

Протокол BB84 является наиболее изученным [39] и простым для реализации подобной системы.

1.4.1 Алгоритм протокола BB84

Структурная схема системы КРК изображена на рис. 1.6, на первом этапе происходит передача сигнальных импульсов по квантовому каналу (КК) между легитимными пользователями А (ПА) и Б (ПБ), в ПОМ происходит приготовление, а в КУ – кодирование состояний, далее в ДУ происходит декодирование, а в ПрОМ – детектирование. После этого по классическому канала производится обмен информацией о номере используемого для кодирования базиса, без раскрытия состояния. При этом считается, что нелегитимный пользователь может прослушивать классический канал, но не может вносить изменения в передаваемые данные, а перехват информационных посылок из квантового канала приводит к возникновению дополнительных ошибок [7, 32].

Механизм защиты основан на случайной смене стороной ПА в каждом такте формируемой ею последовательности кубитов $\mathbf{m}_A$ состояний используемого для их приготовления вычислительного базиса. Альтернативные состояния базиса $|0\rangle$-$|1\rangle$ и $|0'\rangle$-$|1'\rangle$ в различных тактовых интервалах $\mathbf{m}_A$ при этом оказываются развернутыми друг относительно друга на фиксированный угол $\varphi=45^0$ [7, 15, 39]. В целом система при этом ориентирована на проведение стороной ПБ проекционных измерений кубитов (измерений фон Неймана), т.е измерений с четким исходом, при которых **A** представлен проектором *i*- го кубита из $\mathbf{m}_A$ на кет-векторы соответствующего вычислительного базиса. С этой целью при приготовлении $\mathbf{m}_{Ai}$ в любом из альтернативных базисов $|0\rangle$-$|1\rangle$ или $|0'\rangle$-$|1'\rangle$ один коэффициентов α, β в (1), в зависимости от значения передаваемого символа (0 или 1), всегда обращается в ноль.

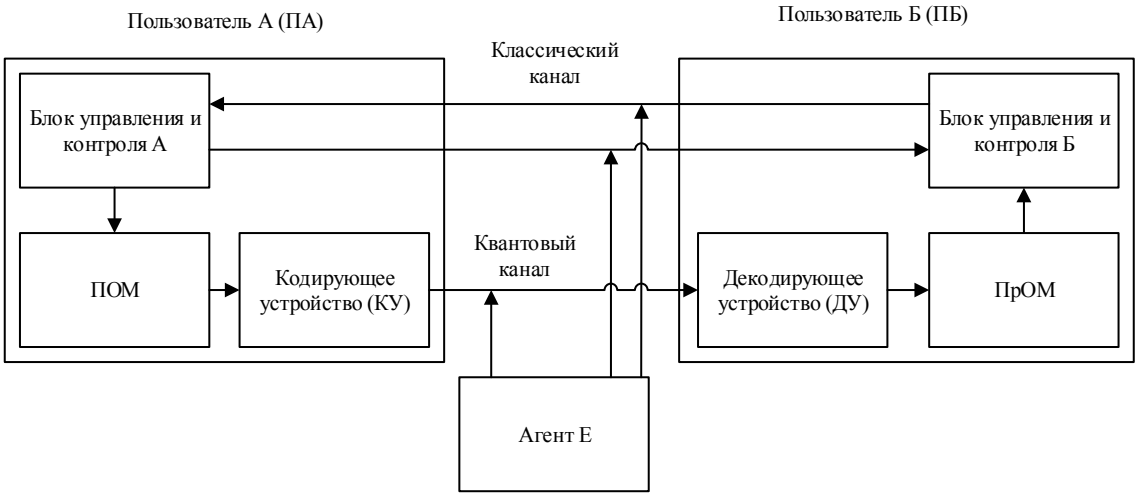


Рис. 1.6. Структурная схема системы КРК

Для реализации проекционных измерений, поступающих из квантового канала последовательности $\mathbf{m}_A$. сторона ПБ формирует у себя собственную случайную последовательность $\mathbf{m}_Б$ состояний своего измерительного базиса, состоящую из тех же векторных комбинаций $|0\rangle$-$|1\rangle$ и $|0'\rangle$-$|1'\rangle$. В силу некоррелированности $\mathbf{m}_A$ и $\mathbf{m}_Б$ среднее число совпадения вычислительного и измерительного базисов в указанных последовательностях возможно лишь для половины элементов из

которых и формируется ключевая последовательности $\mathbf{k}_{АБ}$. Для второй половины элементов условия проекционных измерений не выполняются. Здесь измерительный базис $\mathbf{m}_{Бi}$ оказывается повернутым относительно векторов вычислительного базиса ПА данного элемента $\mathbf{m}_{А}$, следовательно, на стороне Б $\mathbf{m}_{Аi}$ оказывается в суперпозиции состояний векторов измерительного базиса $\mathbf{m}_{Бi}$. Формально данная ситуация означает, что оба коэффициента α и β измеряемого кубита $\mathbf{m}_{Аi}$ отличны от нуля, и безошибочное копирование кубитов в данных условиях невозможно в принципе [13]. Согласно ТЗК нелегитимному пользователю Еве, которая осуществляет атаку на канал связи легитимных пользователей системы КРК, не сможет получить из сообщения даже частичную информацию без изменения ее случайным и неконтролируемым образом, что с большой вероятностью будет детектировано ПА и ПБ [7]. Отсюда следует, что перспективы успешного копирования ключевой последовательности $\mathbf{m}_{К}$ агентом Е могут быть связаны лишь с несовершенством программно-аппаратного устройства системы КРК ПА и ПБ. К основным системным показателям такого рода обычно относят уровень ошибок и B - скорость формирования $\mathbf{k}_{АБ}$ (битрейт), которые используются для контроля и детектирования атак АЕ [7, 39].

Теоретическим пределом ошибки, до которого данный протокол является защищенным, составляет около 11% [64]. В случае использования Евой следующих атак: прием-перепосыл, прозрачное индивидуальное подслушивание, коллективной и когерентной атаки данная критическая величина корректна [64].

Однако для атаки с расщеплением по числу фотонов (photon number splitting attack – PNS), которая основана на том, что в системах КРК обычно используются ослабленные лазерные импульсы, вместо строго однофотонных, протокол BB84 является полностью незащищенным [39, 64]. Данная атака сводится к тому, что агент Е неразрушающим образом измеряет в разрыве квантового канала числа фотонов в импульсах. Однофотонные импульсы при этом блокируются, а пользователю Б транслируются только импульсы с двумя и более фотонами, один из которых агент Е сохраняет в своей квантовой памяти. Битовое состояние этого

фотона АЕ может легко установить позднее, после раскрытия и согласования пользователями состояний соответствующих базисов по классическому каналу. АЕ маскирует заблокированные импульсы используя канал связи с меньшим затуханием [39], однако это возможно только при определенной критической длине квантового канала, которая зависит от доли двух- и более фотонных импульсов в передаваемых информационных посылках.

1.4.2 Ограничение на уровень ошибок в протоколе BB84

Рассмотрим ограничения на допустимый уровень ошибок p^* в квантовом канале (КК), при использовании протокола BB84 [64]. При этом будем считать актуальной моделью КК двоичный симметричный канал (ДСК) без памяти [65].

Как известно, в присутствии шума средний битовый объем информации в передаваемых по ДСК символах R_i связан с вероятностью p ошибок их приема, или, соответственно, вероятностью правильного приема - $q=1-p$ как [65]:

$$R_i = 1+(1-p)log_2(1-p)+plog_2p. \quad (1.8)$$

Из (1.8), в частности, следует, что $R(p=0)=1$, а также, что с приближением p к уровню 0,5 средний битовый объем информации в символах КК падает до нуля.

Соотношение (1.8) позволяет оценить допустимый уровень p в КК. Действительно, в соответствии с данным выше описанием протокола BB84, максимальное количество информации, которое нелегитимный пользователь может извлечь из каждого элемента последовательности кубитов $\mathbf{m}_A$ в КК, не превышает половины бита. При этом вторая половина бита будет являться источником дополнительных ошибок p_E, вносимых клон-машиной (КМ) АЕ в КК. Суммарная вероятность ошибок p_Σ в этом случае будет равна:

$$p_\Sigma = p+p_E \quad (1.9)$$

Как отмечалось выше, уровень p_Σ строго контролируется сторонами ПА и ПБ в ходе процедуры КРК. Поэтому для извлечения информации о второй половине бита в элементах $\mathbf{m}_A$, АЕ может замаскировать p_E под естественные шумы канала p, обеспечив равенство $p_\Sigma=p_E$. Для этого он имеет теоретическую возможность

такой реконструкции КК, при которой p=0. Для данного случая допустимый уровень шибок p^* в КК можно найти из уравнения (1.8) для,

$$R=1+(1-p^*)log_2(1-p^*)+plog_2 p^*= 0.5. \quad (1.10)$$

Таким образом, безусловная защищенность КК системы КРК ограничена уровнем коэффициента квантовых ошибок Q-BER≈11%.

1.4.3 Особенности работы протокола B92

Основное отличие от вышеописанного протокола для B92 в том, что для кодирования состояния фотона на передающей стороне используется один базис с двумя неортогональными состояниями – «0» соответствует поляризация 0^0, «1» - 45^0. Измерение при этом происходит в двух базисах: в прямом, где «0» - 0^0, «1» - 90^0 и диагональном, где «0» - 45^0, а «1» - 135^0.

При этом важно отметить, что проекционные измерения, которые выполняются при совпадении передаваемого состояния и базиса для измерения, происходят только для символа «0». Иначе вероятности для появления «0» и «1» составляют 50%.

В том случае, когда ПБ получает в результате измерения «1» - это указывает на то, что он не угадал переданное ПА состояние и соответствующие биты в последовательностях $\mathbf{m}_А$ и $\mathbf{m}_Б$ не совпадают. По классическому каналу пользователь Б сообщает номера битов, где получил «1», пользователю А. После инвертирования одним из пользователей ключевой последовательности, на сторонах ПА и ПБ получаются полностью совпадающие ключи $\mathbf{k}_{АБ}$.

ТЗК не допускает точного копирования неизвестного квантового состояния, однако возможно создание клон-машиной нелегитимного пользователя неидеальных копий, для этого используются так называемые POVM-измерения [13] или измерений с тремя исходами [39]. В результате возможно два определенных исхода:

$$M_0 = \frac{I - |\psi_1\rangle\langle\psi_1|}{1+\cos\eta},$$

$$M_1 = \frac{I - |\psi_0\rangle\langle\psi_0|}{1+\cos\eta}$$

и одно неопределенное: $M_? = I - M_0 - M_1$. Причем величина последнего зависит от значения угла η между неортогональными состояниями внутри базиса. Чем он ближе к π/2, тем меньше неопределенных исходов измерений и тем ниже стойкость против перехвата, однако при этом увеличивается скорость передачи, например, для π/2 $M_?$ = 0, для π/4 $M_?$ = 75%, π/6 $M_?$ составляет около 88% [66].

Атаке с блокированием части импульсов подвержен и протокол B92. Для него атака возможна даже в случае использования строго однофотонного источника – достаточно блокировать принятые состояния с неопределенными исходами, т.е. он является еще более уязвимым для подобного прослушивания, чем BB84 [39].

1.4.4 Стратегии измерений кубитов нелегитимным пользователем

Рассмотрим возможные подходы к созданию программно-аппаратных устройств, используемых нелегитимным пользователем для копирования ключевой последовательности $\mathbf{k}_{АБ}$ в системе КРК. В дальнейшем такие устройства будем обозначать как клон-машина (КМ) [67]. Как указывалось ранее, КМ должны обеспечивать максимально корректные измерения не ортогональных состояний КЧ. Перечислим основные физические ограничения на указанные измерения.

Квантовая теория оптимального измерения двух, в общем случае не ортогональных, квантовых состояний с векторами $|\psi_\pm\rangle$ дает оценку минимальной вероятности ошибки в их идентификации, как:

$$P_?(opt) = \frac{1}{2}\left(1 - \sqrt{1 - 4\eta_+\eta_- \left|\langle\psi_+|\psi_-\rangle\right|^2}\right), \qquad (1.11)$$

где $\eta_\pm$ - априорные вероятности указанных состояний.

Соотношение (1.11) называется границей Хелстрома [68]. Как видим, результат измерений Хелстрома векторов $|\psi_\pm\rangle$ в рассматриваемом случае

ограничен только двумя исходами, характеризуемыми некоторой вероятностью не корректных измерений.

В другом, альтернативном к описанным выше измерениям Хелстрома, способе дискриминации не ортогональных состояний $|\psi_{\pm}\rangle$, так называемом, методе обобщенных измерений, результатом измерений является три исхода. Два из этих исходов являются корректными результатами измерений состояний $|\psi_{\pm}\rangle$, а третий, с вероятностью $P_?$ дает не определенный результат измерения состояния КЧ [69] и показано, что при этом достижимый минимум величины $P_?$ составляет:

$$P_?(opt) = \left|\langle \psi_+ | \psi_- \rangle\right|,$$

и называется границей Ivanovic-Dieks-Peres (IDP). В [70] экспериментальное подтверждение IDP-границы в методе обобщенных измерений состояний $|\psi_{\pm}\rangle$.

1.5 Способы кодирования в системах КРК

1.5.1 Поляризационное кодирование

Рассмотрим принцип работы BB84 на примере первого предложенного протокола КРК [32], в котором $|0\rangle$, $|1\rangle$ выражаются через два состояния поляризации поступательного движения фотона. Такая частица рассматривается как поляризационный кубит (ПК) (polarization qubit) [71].

Обычно пары состояний с поляризационным кодированием используют либо прямые с вертикальным (0°) и горизонтальным (90°) состояниями, либо диагональными 45° и 135°; либо разнонаправленные круговые поляризации. Любые два из этих базисов могут быть использованы в протоколе. Ниже используются прямой и диагональный базисы.

Первым шагом в BB84 является квантовая передача. ПА создает случайный бит (0 или 1), а затем случайным образом выбирает один из двух базисов (прямолинейный или диагональный), чтобы передать его. Затем она готовит состояние поляризации фотона в зависимости от значения бита в базисе. Так, например, 0 кодируется в прямолинейной основе (+) в виде вертикального состояния поляризации, и 1 кодируется в диагональной основе (x) в виде 135 °

состоянии. ПА затем передает один фотон в указанном состоянии ПБ используя квантовый канал. Процесс выбора базиса случаен, ПА записывает состояние, базис и время отправки каждого фотона.

Согласно квантовой механике (в частности, квантовой неопределенности), невозможно измерение с различением 4 различных состояниях поляризации, когда они не все ортогональны. Возможно только измерение между любыми двумя ортогональными состояниями (ортонормированный базис). Так, например, измерения в прямом базисе дает результат по горизонтали или по вертикали. Если фотон был создан с горизонтальной или вертикальной поляризацией (прямой базис), то произойдет правильное измерение состояния, но если он был создан как 45 ° или 135 ° (диагональный базис), то прямое измерения выдает горизонтальное или вертикальное состояние наугад. Кроме того, после этого измерения вся информация об изначальной поляризации фотона будет потеряна.

Так как ПБ не знает базис фотона, все, что он может сделать, это выбрать базис для измерения наугад либо прямой или диагональный. Он делает это для каждого принятого фотона, записывая время, результат измерения и использованный базис. После приема всех фотонов ПБ общается с ПА по публичному классическому каналу. Пользователь А передает какой базис был использован для каждого отправленного фотона, а пользователь Б базис, который он использовал для измерения. Они оба отбрасывают фотоны (биты), где ПБ использовал другой базис, что составляет половину от общего количества переданного ключа, оставляя половину битов в качестве общего ключа.

Структурная схема системы изображена на рис. 1.6. Пользователь А отправляет слабые импульсы с одного из четырех лазерных диодов, излучение каждого из которых поляризуется в строго определенном состоянии. Пройдя через систему светоделителей и квантовый канал, фотон попадает на проходит через светоделитель 50/50 на стороне ПБ – таким образом происходит рандомизация выбираемого для измерения базиса.

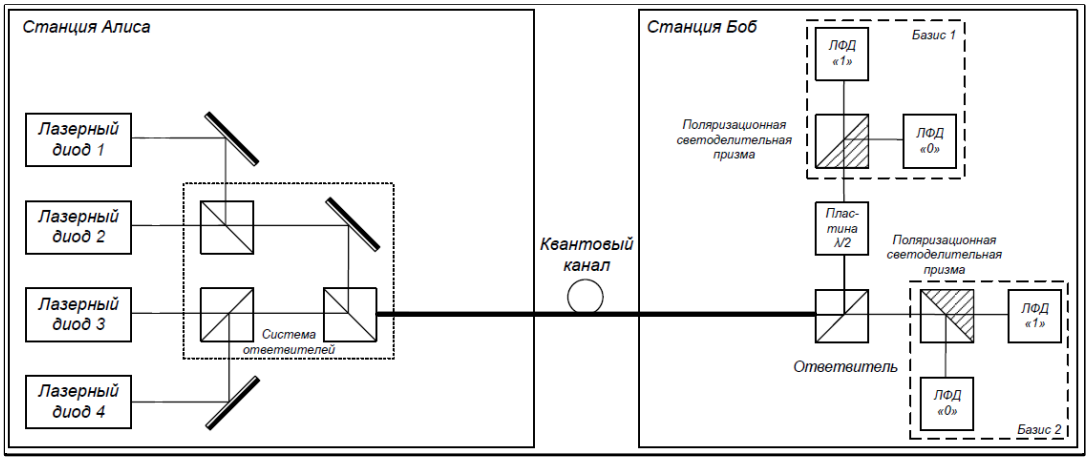


Рис. 1.6. Структурная схема поляризационного кодирования систем КРК

Для проверки на наличие подслушивания, ПА и ПБ сравнивается определенное подмножество их оставшихся битовых строк. Если нелегитимный пользователь получила информацию о поляризации фотонов, это вносит ошибки в измерения ПБ. В случае превышения порогового уровня в 11% [64], пользователи А и Б прекращают общения, т.к. возможно наличие в канале связи агента Е.

Существенным фактором, препятствующим применению ОВ для поляризационного кодирования, является поляризационная дисперсия волокна [71], приводящая к декогеренции ПК в ОВ, т.е. быстрому разрушению когерентных состояний (1). Поэтому использование ПК в ОВ нежелательно.

1.5.2 Фазовое кодирование

Принцип работы фазового кодирования основан на использовании эффекта интерференции амплитуд вероятности. С помощью двух интерферометров Маха-Цендера, один из которых установлен на стороне ПА (ИМЦ-А), а другой на стороне ПБ (ИМЦ-Б) с установленными в плечах фазовые модуляторы (ФМ) достигается конструктивная и деструктивная интерференция, которая фиксируется с помощью двух ПрОМ, подключенных к выходным портам ИМЦ-Б.

При этом квантовое состояние $|\psi\rangle$ на выходе обеих интерферометров в общем случае следует рассматривать как четырехуровневое, а соответствующий вектор

$|\psi_4\rangle$ - как кукварт. Однако при идентичных конструкциях интерферометров два из четырех возможных состояний $|\psi\rangle$ оказываются вырожденными. При этом размерность вектора состояний одиночного фотона на выходных портах ИМЦ-Б снижается до 3, а объект $|\psi_3\rangle$ следует рассматривать уже как кутрит [11]. Форма представления такого объекта аналогична (1.1),

$$|\psi_3\rangle=\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle,$$

где $|0\rangle$, $|1\rangle$, $|2\rangle$ и α, β, γ – кет-векторы состояний и амплитуды вероятности данных состояний кутрита соответственно. Нижний индекс здесь, как и ранее, указывает на число состояний $|\psi_3\rangle$.

Информационным состоянием кутрита является вырожденное состояние $|1\rangle$. Физическими условиями вырождения является равенство суммарной оптической длины L_1 короткого плеча ИМЦ-А и длинного плеча ИМЦ-Б с аналогичной суммой L_2 длинного плеча ИМЦ-А и короткого плеча ИМЦ-Б. Условие балансировки системы из двух разбалансированных интерферометров $L_1=L_2$ дает возможность квантовой частице в состоянии $|1\rangle$ интерферировать сама с собой [1]. Результаты данного эффекта проявляются в форме интерференции вероятностей в состоянии $|1\rangle$.

Передающая сторона использует один из четырех возможных фазовых сдвигов 0°, π/2 – для символа «0», что соответствует первому базису Б-1 а π, 3π/2 – для «1», что соответствует второму Б-2 (рис. 1.7). Выбор базиса для измерения на стороне ПБ происходит за счет сдвига фазы на 0° для Б-1 или на π/2 для Б-2. При этом в случае совпадения базисов пользователей А и Б и детектирования фотона с помощью Д0, ему присваивается значение бита «0», а в Д1 – значение «1», рис. 1.5. [7].

Особенностью систем с фазовым кодированием является то, что для корректной работы необходима точная подстройка разности оптических путей интерферометров с точностью до долей длины волны [7, 15], в криптосистемах с самокомпенсацией «Plug&Play» для этих целей используются фарадеевские зеркала [7].

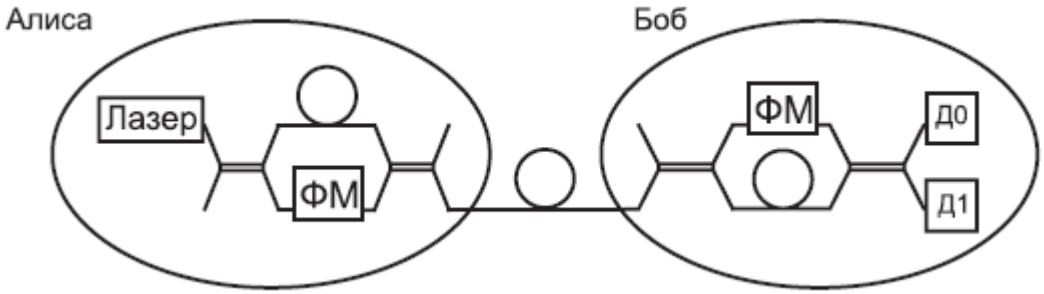


Рис. 1.7. Структурная схема фазового кодирования систем КРК

1.5.3 Временное кодирование

Наибольшую устойчивость однофотонных состояний $|\psi\rangle$ к динамическим флуктуациям параметров оптоволоконного квантового канала связи обеспечивает метод временного кодирования (ВК) $|\psi\rangle$, при котором кодовое состояние (0 или 1) одиночных фотонов определяется их положением относительно заданных кодовой таблицей временных промежутков (тайм-слотов) тактового интервала [72, 72]. Простейшая процедура приготовления таких состояний состоит в применении стороной ПА время-импульсной модуляции излучения лазера [72, 73], а оценка их кодового состояния - в измерении ПБ моментов срабатывания регистрирующих квантовые частицы его фотоприемными устройствами относительно границ тайм-слотов [72, 72, 73].

Рассмотрим один из вариантов ВК, предложенного Молотковым С. Н. в 2004 году (М04) [72]. В нем используется два базиса, в каждом из которых по два подбазиса, (рис. 1.8) временные интервалы между ними попарно неортогональны, а между +(1) и ×(1), +(2) и ×(2) для одинаковых кодовых состояния ортогональны.

Для передачи состояния фотона на стороне ПА в начале случайным образом выбирается базис, подбазис и значение бита «0» или «1». На приемной стороне происходят измерения в случайно выбранных временных интервалах $\Delta 1 \ldots \Delta 5$. После окончания передачи по квантовому каналу, приемная сторона сообщает передающей в каких тайм-слотах были детектированы информационные посылки, а та в свою очередь раскрывает использованный базис и подбазис.

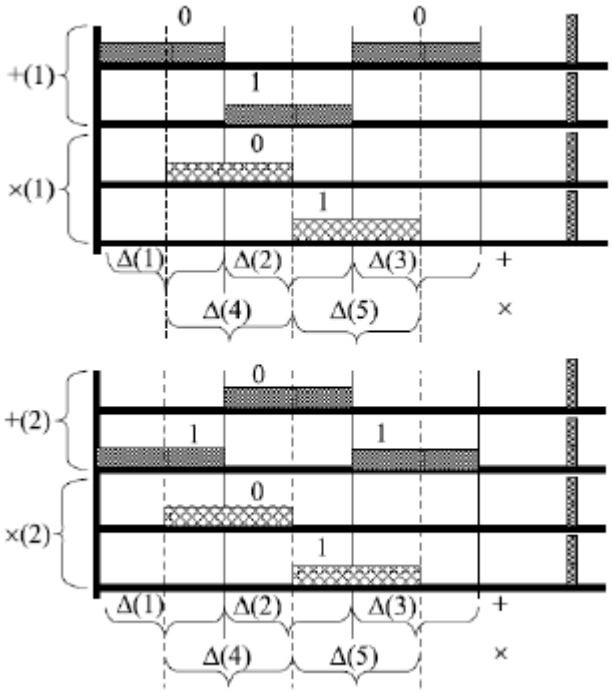


Рис. 1.8. Кодовые состояния базиса для временного кодирования M04

Измерения состояний в данном случае, фактически, всегда являются проекционными, поскольку исключают неоднозначные оценки временного положения одиночного фотона в квантовом канале. Как отмечалось, именно неоднозначность измерений состояний $|\psi\rangle$ при не совпадающих базисах – измерительном и базисе, использованном для приготовления кубита, обеспечивает основной уровень защиты протокола КРК. Она заставляет нелегитимную сторону АЕ проводить нечеткие измерения последовательности $\mathbf{m}_{A,}$ совершать собственные ошибки, которые затем детектируются в общем уровне ошибок.

Отмеченная особенность метода существенно снижает защищенность системы, а применение временного кодирования состояний квантовых частиц для организации КРК-ВК требует других, дополнительных способов защиты протокола.

Одним из вариантов решения проблемы уязвимости системы КРК может быть внедрение в последовательность сигнальных посылок импульсов-ловушек (decoy-states), которые являются многотофотонными [75]. В случае перехвата данных

нелегитимным пользователем, статистика проверочных импульсов изменяется и делается вывод о наличии нелегитимного пользователя в квантовом канале. Уязвимостью данного метода является то, что АЕ может обнаружить импульсы-ловушки по отличному от сигнальных среднему числу фотонов.

Развитие метода обнаружения нелегитимного пользователя по средствам внедрения decoy-states получило в работе [75, 76] и методе кодирования [77] с тем же средним количеством фотонов.

Рассмотрим последний более подробно. Принципиальная схема установки системы КРК представлена на рис. 1.9, где 1 – компьютер ПА, 2 – лазерный источник импульсного излучения, 3 – аттенюатор оптического оптического излучения, 4 – расширитель пучка, 5 – атмосферный канал, 6 – телескоп, 7, 9 – делители пучка, 8 – разбалансированный интерферометр Маха-Цендера, 10 – детектор одиночных фотонов (Д0 – сигнальный), Д1 и Д2 – контрольные), 11 – измеритель временных интервалов, 12 – компьютер ПБ, 13 – классический канал. На рис. 1.10 изображены – а) сигнальные импульсы, б) многофотонный синхронизирующий импульс. ПА пересылается одно из 4 возможных состояний. На приемной стороне световой поток делится на две равные части с помощью светоделителя, одна часть подается на сигнальный детектор, а часть – на в блок контроля когерентности, содержащий интерферометр Маха-Цендера на выходных портах которого установлены детекторы Д1 и Д2. Разность плеч ИМЦ составляет $T/2$. Как пишут авторы: «Импульс длительностью T разбивается в интерферометре на два половины, следующие по длинному и короткому плечам, причем на выходе передняя часть одной половины импульса интерферирует с задней частью другой». Однако практическая реализация с использованием данного принципа представляется достаточно сложной.

Вместе с тем, отмеченный недостаток систем КРК-ВК может быть устранен за счет использования интерферометрического и статистического контроля. Для изучения работоспособности данного предложения необходимо разработать

программную модель как системы с временным кодированием М04, так и подсистем интерферометрического и статистического контроля.

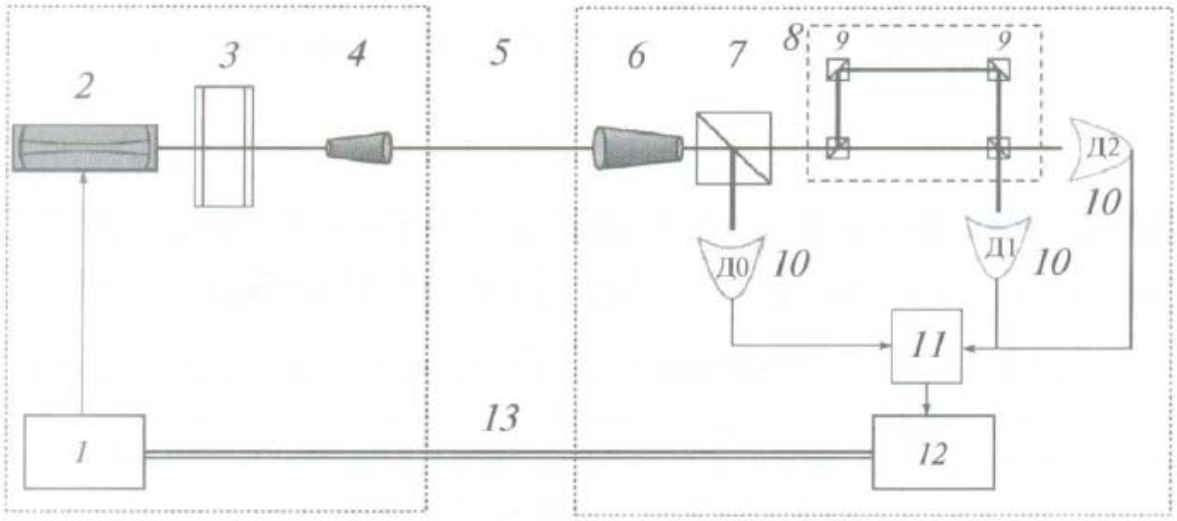


Рис. 1.9. Структурная схема временного кодирования с использованием состояний-ловушек

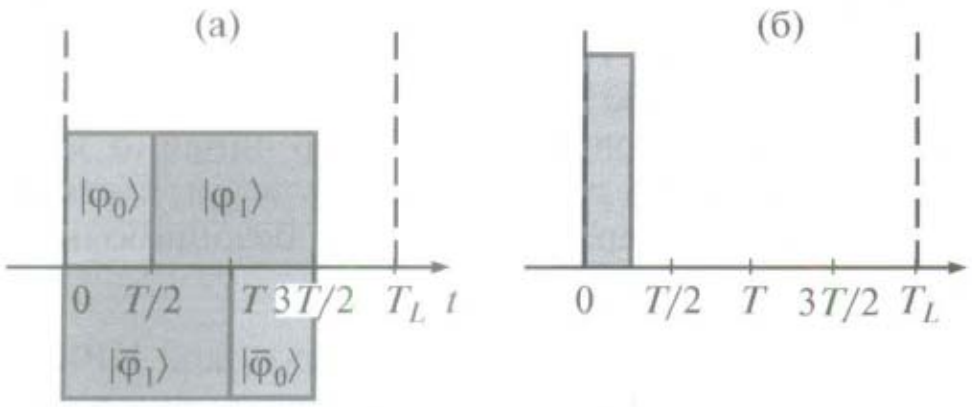


Рис. 1.10. Кодовые состояния базисов для временного кодирования с использованием состояний-ловушек

Другим решением данной проблемы может быть замена применяемых в них одноуровневых состояний $|\psi\rangle$ на двухуровневые tb-кубиты $|\psi_2\rangle$ [31]. Приготовление последних сопряжено с задержками одиночного фотона в

разбалансированном интерферометре Маха-Цендера (ИМЦ), при этом векторы $|0\rangle$, $|1\rangle$ ассоциируются с двумя сдвинутыми во времени состояниями на выходе ИМЦ.

1.6 ПОМ в системах КРК

В соответствии со структурной схемой системы КРК на рис. 1.6, ее передающий оптический модуль (ПОМ) предназначен для приготовления состояния квантовой частицы.

Рассмотрим условия приготовления смесей в обычном лазерном диоде (ЛД) [19, 79]. Для этого воспользуемся уравнением для вероятности распределения фотонов $p(n)$, полученным в рамках квантовой теорией лазера [19]:

$$\dot{p}(n) = -\left[\frac{(n+1)A}{1+(n+1)B/A}\right]p(n) + \left(\frac{nA}{1+nB/1}\right)p(n-1) - \\ -Lnp(n) + L(n+1)p(n+1). \tag{1.12}$$

где A, B - коэффициенты линейного усиления и насыщения активной среды ЛД соответственно; L - потери в резонаторе ЛД.

Рассмотрим решения (1.12) для двух крайних режимов работы ЛД. Если ЛД работает в режиме существенно выше порогового уровня ($A>>L$), решение уравнения (1.8) имеет вид указанной выше пуассоновской статистики (1.7) где $\langle n\rangle = A/BL$. Можно показать, что дисперсия числа фотонов Δn^2 распределения (1.7) равна [3,5,7]:

$$\Delta n^2 = \langle n\rangle. \tag{1.13}$$

На пороге генерации, когда $A=L$ в линейном приближении ($B=0$) уравнение (1.12) для $p(n)$ в стационарном состоянии ($p(n)=0$) имеет классическое решение,

$$p(n) = \left[1-\exp\left(-\frac{\hbar}{k_B T}\right)\right]\exp\left(-\frac{\hbar}{k_B T}\right), \tag{1.14}$$

описывающие излучение черного тела с абсолютной температурой T.

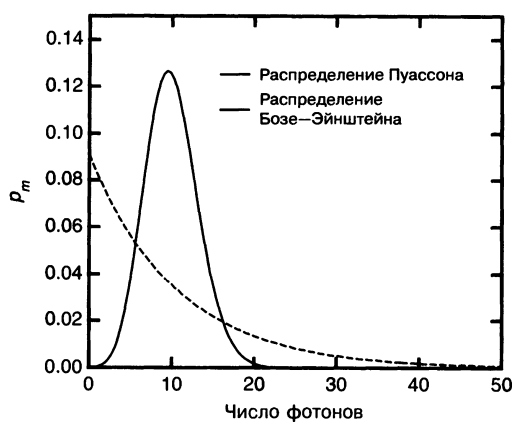
Распределение отсчетов фотонов $p(n)$ для указанного источника хаотического света зависит также от соотношения длительности светового импульса τ и его

времени когерентности τ_c. При $\tau \ll \tau_c$ (короткие импульсы) мгновенное число квантов излучения в течение τ постоянно. Распределение вероятности $p(n)$ для мгновенного числа квантов хаотического света находится путем усреднения (1.10) по времени. В результате получим статистистическое распределение Бозе-Эйнштейна [19, 24]:

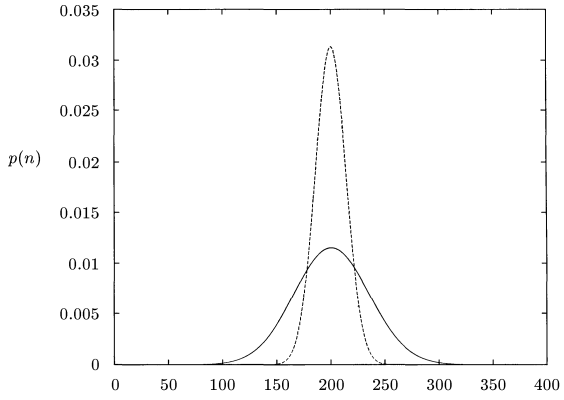
$$p(n) = \frac{1}{1+\langle n \rangle}\left(\frac{\langle n \rangle}{1+\langle n \rangle}\right)^n \tag{1.15}$$

В случае, когда время когерентности τ_c превышает τ, ($\tau \gg \tau_c$) соотношение (1.15) переходит в пуассоновское распределение (1.7).

В промежуточном режиме, между порогом генерации ($A=B$) ЛД и условием ($A \gg L$), решение уравнения (1.12) находится путем численного расчета. В указанной области нормированная дисперсия Δn^2 распределения фотонов описывается параметром Манделя ξ [19, 24]:

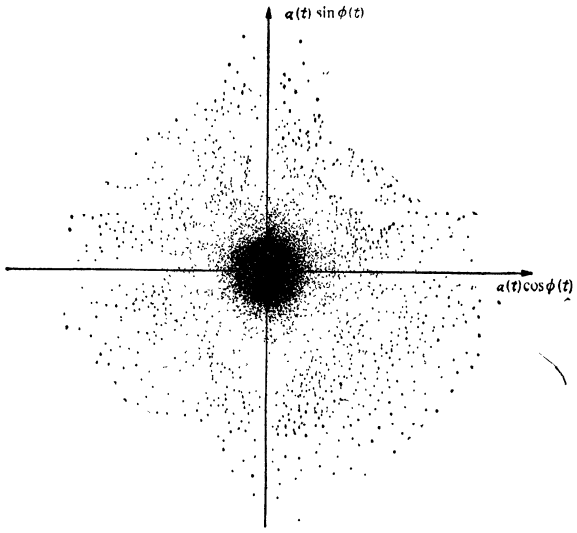


а. Сравнение распределений Пуассона и Бозе-Эйнштейна для среднего числа фотонов в резонаторе, равного десяти.

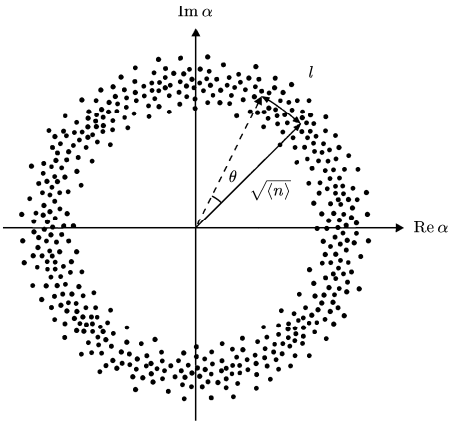


б. Функция распределения фотонов в когерентном (точки) и лазерном (сплошная линия) состояниях с 20% превышением порога генерации

Рис. 1.11 Сравнение распределений вероятности



а. Распределение вероятностей для амплитуды и фазы электрического поля хаотического светового пучка.



б. Представление напряженности электромагнитного поля на комплексной плоскости. Фаза диффундирует вследствие спонтанного излучения

Рис. 1.12 Структуры напряженности электрического поля

$$\xi = \frac{\left\langle n^2 \right\rangle - \left\langle n \right\rangle^2}{\left\langle n \right\rangle} - 1 = \frac{L}{A - L} \tag{1.15}$$

Поскольку здесь $A>L$, то параметр Манделя $\xi>0$, что указывает на суперпуассоновский характер распределения $p(n)$ [24]. При увеличении тока инжекции значительно выше порогового уровня ($A>>L$) величина ξ в формуле (1.15) стремится к нулю, а $p(n)$ к пуассоновскому распределению.

Сравнивая формулы (1.11) и (1.14), видим, что распределение Бозе-Эйнштейна намного шире пуассоновского распределения. Взятые из [79] графики на рис. 1.11 иллюстрирует эти различия. На рис. 1.11 (а) представлены зависимости $p(n)$, рассчитанные для среднего числа $\langle n\rangle$ фотонов в состоянии $|\alpha\rangle$, равного десяти. Данные на рис. 1.11 (б) демонстрируют переход статистики когерентных

состояний $|\psi\rangle$ от пуассоновской к суперпуассоновской по мере снижения тока инжекции ЛД и приближения его к пороговому уровню I_{th}.

Различие структуры напряженности электрического светового поля теплового происхождения ($A=L$) и когерентного светового поля ($A>>L$) показано на рис. 1.12 [24].

Приведенное выше описание особенностей статистики фотонов

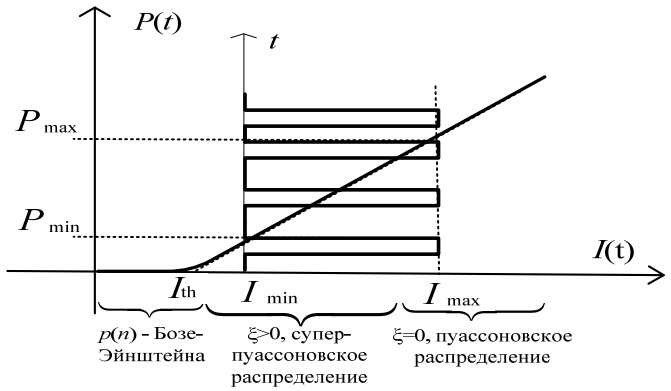


Рис. 1.13. Изменение $p(n)$ при модуляции $I(t)$ ЛД относительно уровня порогового тока I_{th}

лазерного излучения указывают на изменение распределения $p(n)$ при модуляции тока инжекции $I(t)$ ЛД цифровой двоичной последовательностью. На ватт-амперной характеристике ЛД, представленной на рис. 1.13, можно выделить три области уровней тока инжекции $I(t)$ ЛД в которых реализуются перечисленные выше типы статистик $p(n)$. В первой области, расположенной вблизи порогового тока I_{th}, излучение ЛД близко к тепловому, а $p(n)$ описывается формулой (1.14). В надпороговом режиме ЛД распределение $p(n)$ сжимается и становится суперпуассоновским. При значительном превышении $I(t)$ уровня порогового тока I_{th} лазер генерирует чистые когерентные состояния $|\alpha\rangle$ с параметром Манделя $\xi=0$. Отсюда следует, что для исключения зависимости статистических свойств, приготавливаемых в ПОМ состояний $|\psi\rangle$ от уровня кодирующего сигнала $I(t)$ необходимо отказаться от простой модуляции ЛД током инжекции. Для этого

необходимо обеспечить режим непрерывной генерации в ЛД когерентных состояний $|\alpha\rangle$ при постоянном токе инжекции $I_0 >> I_{th}$. Необходимое для реализации протокола КРК кодирование внутренних параметров $|\alpha\rangle$ при этом может осуществляться помощью внешних аппаратных устройств, таких, например, как электрооптические модуляторы (ЭОМ) [79].

1.7 ПрОМ в системах КРК

На аппаратном уровне основные особенности системы КРК сосредоточены в оптоэлектронных блоках системы и, прежде всего, в контроллерах датчиков ПрОМ. В качестве таковых на практике наибольшее распространение получили лавинные фотодиоды (avalanche photodiode (APD)) [80, 81, 83] в силу наилучших параметрах при детектировании слабых оптических сигналов.

1.7.1 ПрОМ с использованием ЛФД в линейном режиме

В линейном режиме работы фотодиода при подаче большого обратного напряжения, близкого к уровню лавинного пробоя, происходит увеличение фототока из-за ударной ионизации. Увеличения энергии электрона приводит к превышению порога ионизации, в следствии этого при столкновении с электроном из валентой зоны происходит возникновение новой электронно-дырочной пары, а те могут служить причиной возникновения новых носителей заряда [83].

Основными шумами, связанными с подобными фотодатчиками, являются дробовые, шумы темнового тока и поверхностные шумы тока утечки [83].

Наименьшими шумами обладают кремниевые ЛФД. В силу работы со слабыми оптическими сигналами даже незначительное ухудшение отношения сигнал-шум может серьезно повлиять на результат, поэтому для источника питания диода необходимы минимальные пульсации напряжения с целью поддержания стабильности рабочей точки. Фактором, усложняющим разработку источника, является то, что необходимое напряжения питания достаточно велико – порядка 400 В.

Имеющиеся в продаже образцы, удовлетворяющие данным требованиям, вследствие универсальности, обладают большими габаритами и высокой стоимостью. Поэтому принято решение о разработке специализированного, малогабаритного источника питания.

1.7.2 ПрОМ с использованием ЛФД в гейгеровском режиме

Новые возможности в достижении предельной скорости формирования ключа и чувствительности ПрОМ открывают лавинные фотодиоды специальной конструкции G-SPAD (Single Photon Avalanche Diode), способные работать в ключевом режиме, который в литературе называется гейгеровским [80, 81]. В гейгеровской моде напряжение питания диода U_a превышает пороговое напряжения U_b лавинного пробоя на величину так называемого перенапряжения (U_a.- U_b). В этих условиях возбуждение G-SPAD единичным фотоэлектроном приводит к формированию в *p-n* переходе диода лавинного процесса с глубокой внутренней положительной обратной связью, приводящего без дополнительного усиления к формированию в нагрузке G-SPAD сигнального отклика i_s в несколько вольт. На этом фоне внутренние шумы ПрОМ оказываются пренебрежимо малыми.

Механизмы возникновения ошибок в системе (пропуски сигнала и ложные срабатывания ПрОМ) в ключевом режиме G-SPAD являются эффекты афтерпалсинга и спонтанного формирования лавин электронами темнового тока i_{tt}, который при перенапряжении перехода диода трансформируется в хаотическую последовательность коротких импульсов [80, 82].

Для реализации преимуществ G-SPAD по чувствительности и быстродействию требуется решение ряда схемотехнических задач. Для снижения влияния афтерпалсинга и DCR на помехоустойчивость системы контроллер G-SPAD должен обеспечивать импульсный режим работы диода, называемый временным стробированием (Time-gated single photon counting - TGSPC), при котором питание (U_a-U_b) подается на диод лишь в течении короткого времени τ~1нс с частотой B_0 [1,6]. Сложность этой задачи связана с необходимостью формирования TGSPC-

импульсов большой скважностью ($(B_0 \cdot \tau)^{-1} \sim 10^7$) и минимальным джиттером. Кроме этого амплитуды формируемых контроллером G-SPAD постоянного напряжения U_b и импульсного перенапряжения (U_a-U_b) должны быть регулируемыми и для некоторых типов G-SPAD пределы этой регулировки могут составлять несколько сот вольт.

1.8 Особенности помехоустойчивости систем КРК

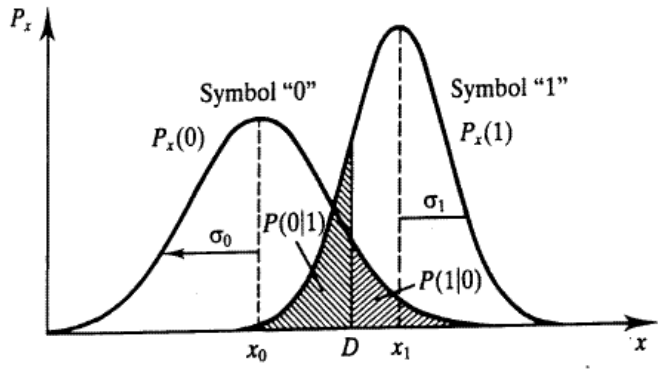


Рис. 1.14. Плотности вероятности напряжения для «0» и «1»

Для оценки помехоустойчивости в цифровых системах передачи данных используется коэффициент битовых ошибок BER [83]. При этом строятся плотности вероятности напряжения на входе пороговой схемы для «0» $P_x(0)$ и «1» $P_x(1)$, пример изображен на рис. 1.14.

Порог срабатывания решающей схемы выставлен таким образом, чтобы минимизировать вероятность принятие неверного решения о значении переданного символа, т.е. $P(1|0)$ и $P(0|1)$.

В системах КРК кодовый символ передается по средствам кодирования состояния фотона, т.е. нет разницы между переданным «0» и «1» в смысле уровня напряжения на входе пороговой схемы. Для систем КРК необходимо соблюдение определенного критического уровня ошибок, а не его минимизация. Таким образом, критерии для оценки помехоустойчивости для стандартных цифровых систем и систем КРК различны, последние необходимо реализовать в качестве

модели оценки помехоустойчивости с целью обеспечения работоспособности по средствам соблюдения критического уровня ошибок.

1.9 Выводы по главе и постановка задачи

В соответствии с приведенным выше литературным обзором систем КРК с временным кодированием, реализация цели настоящего диссертационного исследования связана с решением следующих задач:

1. Разработка расчетной и программной моделей оценки помехоустойчивости ПрОМ и скорости генерации ключа системы КРК с целью контроля вероятности ложного сигнала, от уровня которой зависит защищенность системы.
2. Разработка контроллера ЛФД для линейного и гейгеровского режимов работы ПрОМ.
3. Разработка схемы и модели процесса приготовления многоуровневых временных состояний квантовых частиц с помощью нескольких интерферометров Маха-Цендера.
4. Разработка схем и моделей подсистем интерферометрического и статистического контроля, а также модели системы КРК с временным кодированием одноуровневых состояний одиночных фотонов по протоколу BB84, верификация этих моделей и исследование эффективности их применения для защиты системы.
5. Разработка, исследование и верификация метод временного кодирования двухуровневых временных однофотонных состояний, приготавливаемых в разбалансированном интерферометре Маха-Цендера, для построения оптоволоконной системы КРК.

2. ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ И СХЕМОТЕХНИКА ПРОМ СИСТЕМЫ КРК

Данная глава посвящена решению первых из поставленных диссертационных задач. Здесь рассматривается модель для оценки помехоустойчивости и битовой скорости генерации ключа, показана возможность реализации ПрОМ на основе диода Hamamatsu S8664-05K, предложен высоковольтный источник питания для него, а также предложен контроллер ЛФД в гейгеровском режиме на длинных линиях. Помимо этого, рассмотрена аппаратная платформа системы КРК.

Следуя общей схеме построения систем КРК [7, 15, 80], будем полагать, что в передающем оптическом модуле (ПОМ) приготавливаются неортогональные кодовые состояния фотонов в соответствии с возбуждающей их двоичной псевдослучайной последовательностью (ПСП), формируемой в генераторном блоке G со средней битовой скоростью B_0 (см. рис. 2.1). Также будем считать, что указанные состояния фотонов предназначены для передачи по волоконно-оптической линии (ВОЛС), связывающей блоки ПОМ и ПрОМ (рис. 2.1). Для исключения разрушений в ходе транспортировки по оптическому волокну, будем полагать, что их приготовление в блоке ПОМ осуществляется на основе временного кодирования [72, 72].

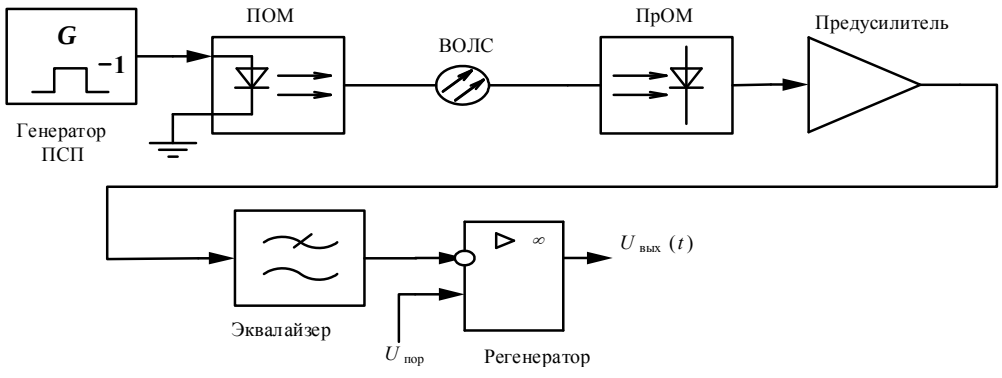


Рис. 2.1 – Структурная схема приемо-передающей части системы КРК

2.1 Оценка помехоустойчивость линейного режима работы ЛФД

Рассмотрим в начале параметры системы КРК в линейном режиме работы APD. Будем считать, что канал КРК построен на основе оптического волокна (ОВ)

длиной L и с погонным затуханием α[дБ/км]. Внутренние шумы предварительного усилителя ПрОМ представим приведенными к входу шумовыми источниками тока и напряжения S_E, S_I (рис.2.2) [83]. Нагрузочный резистор ЛФД и суммарную емкость выходной цепи ПрОМ обозначены как R и C.

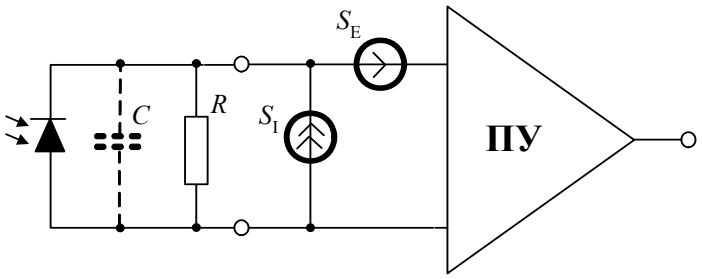


Рис. 2.2 – Эквивалентная схема предварительного усилителя ПрОМ

Как известно, в протоколах КРК ключ $\mathbf{k}_{АБ}$ формируется путем многоступенчатой рандомизации «сырого ключа» $\mathbf{k}_0$ первоначально создаваемого на одном конце канала путем кодирования каких либо неортогональных состояний однофотонных посылок светового сигнала [7, 15, 39]. Обозначим битовую скорость этого исходного ключа как B_0, а среднюю битовую скорость генерации символов секретного ключа - B. Разность значений скоростей B_0-B связана с характеристикой помехоустойчивости приемника КРК – вероятностью генерации ложных символов P_f в ключе $\mathbf{k}_{АБ}$. При отыскании оптимальных схемотехнических решений ПрОМ необходимо контролировать обе указанные зависимости. Рассмотрим каждую из них.

На практике, как уже отмечалось, значение среднего числа фотонов в посылке m берется ~0.1 [72, 72], так, что $p(1)\approx0.1$, а $p(0)\approx0.9$. Это обеспечивает дополнительную рандомизацию последовательности фотонов уже на этапе лазерного излучения.

Другие механизмы случайного удаления однофотонных посылок из последовательности $\mathbf{k}_{АБ}$ в рассматриваемой технологии связаны с поглощением фотонов в оптическом волокне, а также особенностями протоколов КРК. Так в протоколе BB84 коэффициент $k_р$ протокольного снижения скорости B_0 составляет

0.5, а в протоколе B92 для стандартного случая – 0.25 [33]. Результирующая ключевая последовательность $\mathbf{k}_{АБ}^{*}$ в дальнейшем формируется сторонами А и Б в результате применения к «сырому» ключу [7] $\mathbf{k}_{АБ}$ процедуры коррекции ошибок [6].

Еще один фактор снижения B обусловлен внутренними шумами ПрОМ, которые, с одной стороны, с вероятностью P_l, приводят к пропускам сигнальных посылок в моменты опроса пороговой схемы, а с другой, с вероятностью P_f - к генерации ложных символов в ключе $\mathbf{k}_{АБ}$. По величине P_l можно получить оценку для скорости B [84]:

$$B = B_0(1-P_l)p(1)k_p 10^{\frac{-(\alpha L)}{10}} \qquad (2.1)$$

Сделаем еще одно допущение, касающееся формы импульсной характеристики $\delta_c(t)$ ЛФД, которую определим как его реакцию на одиночный фотон. Эта реакция определяется, с одной стороны, скоростями процесса лавинной ионизации и дрейфа плазменного сгустка в p–n-переходе, и разряда емкости C выходной цепи ПрОМ – с другой. Обозначим длительность импульса $\delta_c(t)$ как τ_0. Форма отклика $\delta_c(t)$ ЛФД на одиночный фотон приведена на рис. 2.4. Аппроксимируем указанную импульсную характеристику гауссовой кривой:

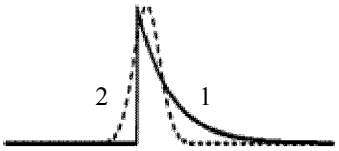


Рис. 2.3 – Форма сигнального тока ЛФД в режиме счета фотонов (1) и гауссова аппроксимация импульсной характеристики ЛФД (2)

$$\delta_c(t) = \frac{u_0}{\sqrt{2\pi\sigma}} \exp\left(-\frac{t^2}{2\sigma^2 T_0^2}\right), \qquad (2.2)$$

где σ – параметр формы импульса, определяющий долю тактового интервала $T_0 = 1/B_0$, занимаемого сигналом $\delta_c(t)$, так, что $\tau_0 = \sigma T_0$.

Воспользовавшись (2.2), определим вероятности P_l и P_f, связанные с внутренними источниками шума ПрОМ. Среди этих источников рассмотрим шумы нагрузки ЛФД, а также внутренними шумами источников S_E, S_I. При этом

распределение плотностей вероятности $p(n)$ числа n фотоэлектронов в нагрузке ЛФД в отсутствии ($u_c = 0$) и присутствии ($u_c = M$) фотона также будем считать гауссовыми:

$$\begin{cases} p(n/u_c = 0) = \dfrac{u_0}{\sqrt{2\pi\sigma}} \exp\left(-\dfrac{n^2}{2\sigma^2}\right), \\ p(n/u_c = M) = \dfrac{u_0}{\sqrt{2\pi\sigma}} \exp\left(-\dfrac{(n-M)^2}{2\sigma^2}\right); \end{cases} \quad (2.3)$$

с безразмерной дисперсией σ [5]:

$$\sigma^2 = \frac{2i_{tt}}{e}\tau I_2(\alpha) + \frac{\tau I_2(\alpha)}{e^2}\left(S_I + \frac{4kt}{R}\right) + S_E\left[\frac{I_2(\alpha)}{R^2} + (2\pi C)^2 \frac{I_3(\alpha)}{\tau e^2}\right]; \quad (2.4)$$

где t – температура в градусах Кельвина; k – постоянная Больцмана; i_{tt} – темновой ток; R – нагрузочное сопротивление ЛФД; $\tau = 1/B$ – длительность импульсной характеристики ПрОМ, обратная ширине полосы частот приемника B.

Коэффициенты I_2, I_3 в формуле (2.4) называются интегралами Персоника и выражается через отношение спектров огибающей оптического сигнала на выходе и входе ПрОМ [83]. Аргументом этих зависимостей является безразмерная нормированная частота $\Omega = \omega/T$:

$$I_2 = \int_0^\infty \left|\frac{H'_{\text{вых}}(\Omega)}{H_{\text{вх}}(\Omega)}\right|^2 d\Omega, \; I_3 = \int_0^\infty \left|\frac{H_{\text{вых}}(\Omega)}{H_P(\Omega)}\right|^2 \Omega^2 d\Omega \quad (2.5)$$

Искомые параметры помехоустойчивости ПрОМ, вероятности P_l и P_f выражаются через формулы (2.3), (2.4) как:

$$P_l = \int_{-\infty}^{U_{\text{пор}}} p(n/u_c = 0)dn, \; P_f = \int_{-U_{\text{пор}}}^{\infty} p(n/u_c \neq 0)dn, \quad (2.6)$$

где $U_{\text{пор}}$ – порог срабатывания приемника, выраженный через число электронов n, проходящих через нагрузку ЛФД за время τ.

Значение P_f определяет среднюю частоту F_r генерации ложных импульсов кода, вызываемых внутренними шумами ПрОМ [84]:

$$F_r = P_f B_0. \quad (2.7)$$

2.2 Оценка помехоустойчивость гейгеровского режима работы ЛФД

Дадим далее оценку P_l и P_f в нелинейном режиме лавинного диода с временным стробированием.

Основной справочной характеристикой чувствительности G-SPAD, определяющей значение P_l, является эффективность регистрации фотонов $\varepsilon=(1-P_l)$, равная вероятности регистрации падающего на фоточувствительную площадку G-SPAD фотона [81]. Величина ε равна:

$$\varepsilon = A \cdot P_G$$

где A – геометрическая эффективность G-SPAD и P_G – вероятность возникновения гейгеровского разряда.

Как отмечалось выше, сигнальный отклик i_s G-SPAD в гейгеровском режиме намного превышает шумы, поэтому формулы (2.4)-(2.6) для расчета вероятностей P_f здесь не применимы. Если обозначить средние частоты генерации ложных символов, обусловленные эффектами афтерпалсинга и *DCR* соответственно как F_{ap} и F_{dcr}, то [84]:

$$P_f = (F_{ap} + F_{dcr}) / B_0 . \qquad (2.8)$$

2.3 Возможность реализации ПрОМ системы КРК на базе ЛФД в линейном режиме

Особенностью оптического приемника системы КРК является малость промежутка времени τ, в котором локализованы сигнальные фотоэлектроны, по сравнению с длительностью тактового интервала $T_0 = 1/B_0$. Как указывалось выше, значение τ определяется уширением импульсной характеристики ЛФД $\delta_c(t)$ τ_0 в тракте ПрОМ в $\zeta = \tau/\tau_0$ раз.

Свобода в выборе τ и ζ дает возможность оптимизации помехоустойчивости приемника за счет соответствующей регулировки указанных параметров. Возможность оптимизации следует из описываемой формулой (2.4) функции σ(α), в которой второй и последний члены показывают противоположные зависимости от τ. В данных условиях, для известных параметров i_{tt}, R, C, S_E и S_I, несложно

отыскать оптимальное значение τ_{opt}, при котором $\sigma(\zeta)$ достигает минимума. Вывод иллюстрируется графиком $\sigma(\zeta)$ на рис. 2.5, рассчитанный по формулам (1.4), (1.5). График получен для ЛФД S8664-05K с параметрами, взятыми из [86]: $\eta = 0{,}78$, $C = 1{,}5$ пФ, $t = 253$ K, $i_{tt} = 0{,}15$ нА, $M = 100$, напряжение смещения диода $U = 380$ В. Номинал нагрузочного сопротивления ЛФД взят равным 5 МОм, а параметры T_0 и τ_0 – 10 мкс и 2 нс соответственно. На практике необходимое значение τ_{opt} достигается за счет соответствующего эквалайзирования АЧХ ПрОМ.

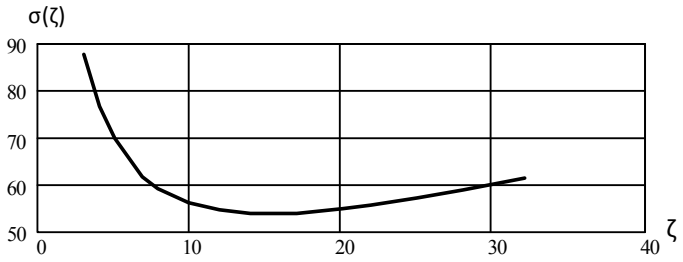


Рис. 2.5 – Зависимость дисперсии шумовых электронов от сжатия $\zeta = \tau/\tau_0$ полосы частот ПрОМ

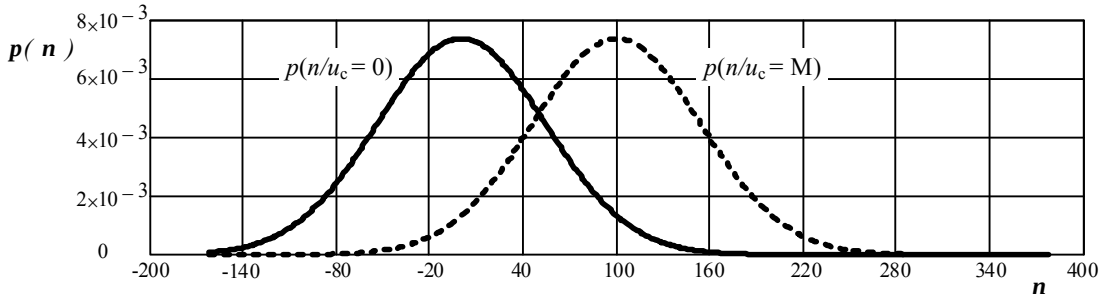


Рис. 2.6 – Зависимость условных плотностей вероятности числа фотоэлектронов в нагрузке ЛФД S8664-05K в отсутствии и присутствии одного фотона

Подставляя полученные данные в (2.3), (2.4) найдем распределения условных плотностей вероятности $p(n/u_c = 0)$ и $p(n/u_c = M)$ числа n фотоэлектронов в нагрузке ЛФД в отсутствии и присутствии фотона. График этих зависимостей приведен на рис. 2.6.

В соответствии с (2.6), расчет параметров помехоустойчивости P_l и P_f, проведем путем интегрирования графиков $p(n/u_c = 0)$ и $p(n/u_c = M)$ в пределах,

ограниченных порогом срабатывания $U_{\text{п}}$. Результаты расчета P_l и P_f как функций $U_{\text{пор}}$ приведены на рис. 2.7.

При анализе данных рис. 2.6 следует учитывать еще одну особенность ПрОМ систем КРК, отличающую их от связных цифровых приемников. Помехоустойчивость последних, как известно, определяется суммой P_l и P_f [83]. Поэтому наилучшим уровнем порога $U_{\text{пор}}$ таких приемников считается точка пересечения кривых $p(n/u_c = 0)$ и $p(n/u_c = M)$ на рис. 2.6. Для систем КРК связь P_l и P_f с помехоустойчивостью более опосредована. Здесь пропущенные символы удаляются из массива $\mathbf{k}_{\text{АБ}}$ в ходе протокольных переговоров, поэтому вероятность P_l не вносит никаких ошибок в формирование ключа, а определяет лишь среднюю скорость B_k его генерации (2.1).

Уровень ложных сигналов в ключе при этом описывается строго контролируемым параметром P_f. В простейшем случае в качестве инструмента контроля может использоваться пороговый уровень $U_{\text{пор}}$. Приведенный на рис. 2.7 пример зависимостей P_l и P_f от $U_{\text{пор}}$ оптического приемника, построенного на ЛФД S8664-05K, вместе с формулой (2.1) демонстрирует возможности управления скоростными параметрами системы и уровнем P_f посредством регулировки $U_{\text{пор}}$, однако при этом основным параметром как уже говорилось выше является величина критического уровня P_f, определяющая секретность передачи данных.

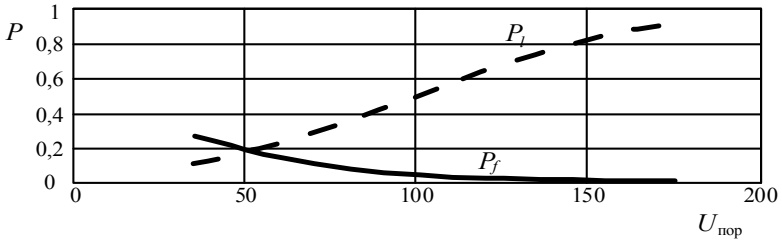


Рис. 2.7 – Зависимости вероятностей P_l и P_f от уровня порога дискриминатора ПрОМ

Представленные расчеты доказывают функциональность рассматриваемой модели ПрОМ при комнатной температуре [87]. При $U_{\text{пор}} = 66$, $P_f = 0{,}11$, длине линии связи 1 км и затухании в оптическом волокне 9 дБ/км скорость генерации ключа будет составлять 2,3 Кб/с. Листинг программной модели расчета помехоустойчивости представлены в Приложении Б.

2.5 Высоковольтный источник питания ЛФД в линейном режиме

Сигнал, после прохождения по волоконно-оптическому тракту, детектируется лавинным фотодиодом и усиливается до необходимого уровня перед подачей на решающее устройство.

В качестве детектора при разработке приемника используется лавинный фотодиод Hamamatsu S8664-05K [86], обладающий низким уровнем темнового тока и высоким коэффициентом усиления, технические характеристики данного диода представлены на рис. 2.8. Согласно графикам, для получения наилучшего значения сигнал-шум необходимо устанавливать напряжение питания как можно ближе к области лавинного пробоя, где коэффициент усиления максимален, но еще не происходит резкого увеличения темнового тока.

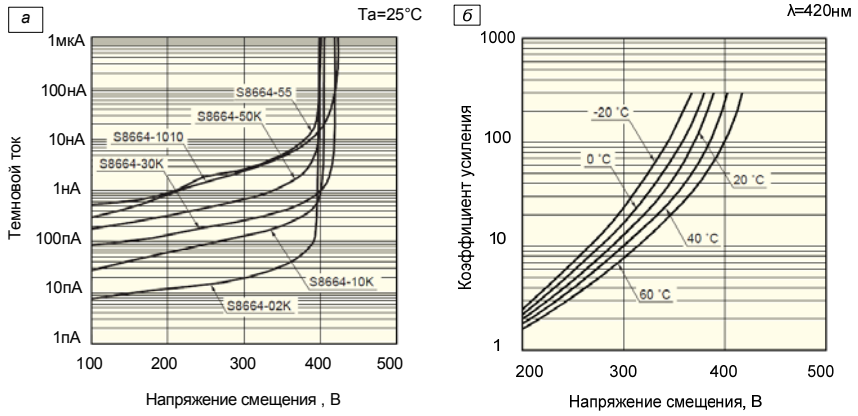


Рис. 2.8 Зависимость темнового тока (а) и коэффициента усиления (б) лавинного диода от величины напряжения смещения [86]

В качестве модели построения выбрана схема повышающего преобразователя, так как она проста в реализации, принципиальная схема представлена на рис. 2.9.

Для исполнения данного схемного решения используется микросхема LM5022 [88], которая обладает рядом преимуществ: имеет отдельный выход для управления ключом, роль которого выполняет транзистор VT_1, а также предусмотрена обратная связь для стабилизации напряжения.

Регулировка выходного напряжения в схеме производится обратной связью, в которую введены 2 потенциометра для грубой и точной подстройки.

Преобразователь напряжения работает в режиме непрерывного тока [89], который предполагает, что энергия, накопленная на индуктивности L_1, расходуется не полностью за один цикл работы преобразователя.

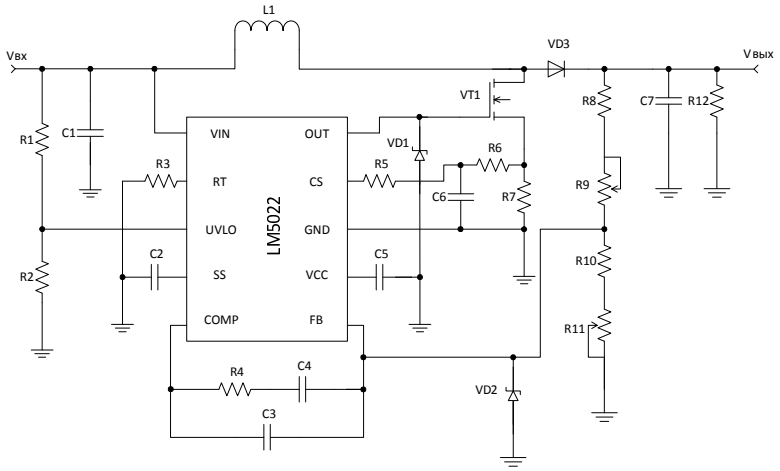


Рис. 2.9 Принципиальная схема источника питания

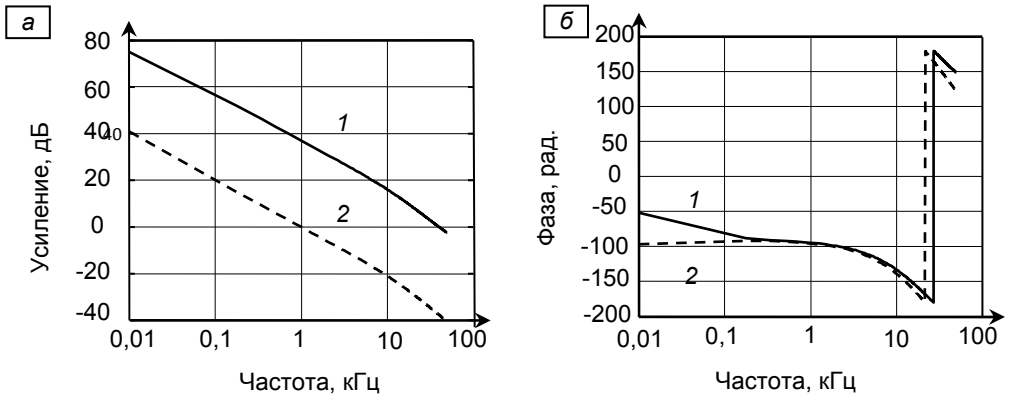


Рис. 2.10 Амплитудно-частотная (а) и фазово-частотная (б) характеристика преобразователя до (1) и после (2) коррекции

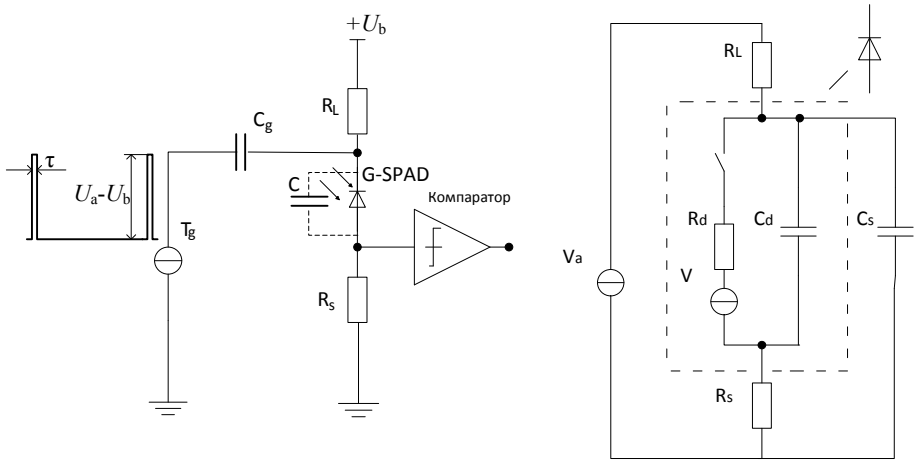
Коррекция частотных характеристик силовой части преобразователя для обеспечения его устойчивой работы, выполнена введением в цепь обратной связи частотно-зависимых элементов C_3 и C_4, частотные характеристики представлены на рис. 2.10.

Таким образом, в данной работе предложена структурная схема фотоприемного модуля для детектирования слабых оптических сигналов, где в

качестве детектора используется лавинный фотодиод Hamamatsu S8664-05K. Для обеспечение необходимого режима работы диода был разработан импульсный источник питания с выходным напряжением до 500 В и пульсациями не превышающими 18 мВ. Выполнен анализ и коррекция частотных характеристик преобразователя с целью обеспечения стабильности его работы [90]. Перечень элементов, которые рассчитывались согласно документации к микросхеме LM5022 [88] и печатная плата представлены в Приложении В.

2.5 Контроллер ЛФД в гейгеровском режиме

Рассмотрим контроллер G-SPAD, обеспечивающий режим временного стробирования диода с пассивным гашением лавины. Функциональная схема устройства представлена на рис. 2.11.



а *б*

Рис. 2.11 *а*- структурная схема контроллера G-SPAD в режиме временного стробирования,
б- схема замещения G-SPAD

Оценка чувствительности ПрОМ в режиме счета фотонов дает среднюю мощность оптического сигнала на входе системы $\sim 10^{-11}$ Вт. Схема пассивного гашения на этом рисунке представлена емкостью C G-SPAD и сопротивлением нагрузки R_L. Номинал R_L выбирается так, чтобы значение постоянной времени $\tau_н = R_L \cdot C$ было сравнительно большим. В этом случае ток лавины на ее начальной стадии разряжает емкость C до напряжения меньшего чем пороговое U_b. Если

время этого разряда $\tau << \tau_н$, то поддерживающая лавинный процесс внутренняя положительная обратная связь диода оказывается разрушенной до момента повторной зарядки емкости и лавина гаснет. В этом режиме диод может рассматриваться как диссипативный ключ, шунтированный статической и динамической емкостями (рис.2.11 б) [80].

Как отмечалось выше, наибольшую сложность в реализации контроллера на рис. 2.11 (а) представляет выбор схемы высокостабильного регулируемого высоковольтного импульсного формирователя перенапряжения T_g, генерирующего короткие стробирующие импульсы с амплитудой (U_a-U_b), частотой B_0 и скважностью $(B_0 \cdot \tau)^{-1}$.

Для решения этой задачи нами предложено использовать в качестве T_g формирователь на разрядных линиях [91]. Принцип работы такого формирователя основан на импульсном преобразовании энергии, накопленной в линии от источника напряжения U_0 при коммутации линии к нагрузке. Накопительная линия ЛЗ в таком формирователе (см. рис. 2.12) сравнительно медленно заряжается от источника постоянного напряжения U_0 через зарядный резистор $R_З$ с номиналом значительно превышающим волновое сопротивление ЛЗ ρ.

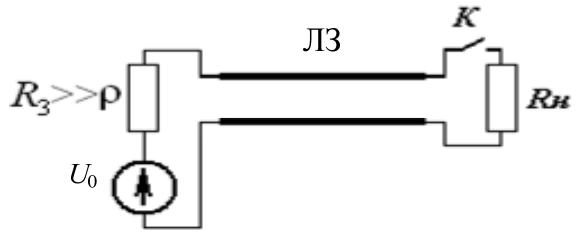


Рис. 2.12 Схема формирователя импульсов с разрядной линией

При замыкании линии ключом K на резистивной согласованной нагрузке формируется прямоугольный импульс напряжения амплитудой:

$$U_H = U_0 R_H / (p + R_H) = U_0 / 2 . \qquad (2.9)$$

Длительность импульса τ_u, формируемого на нагрузке, определяется удвоенным временем прохождения электромагнитной волны по отрезку линии ЛЗ:

$$\tau_u = 2l\sqrt{\varepsilon}/c, \qquad (2.10)$$

где c – скорость света в вакууме; l – длина накопительной линии; ε – относительная диэлектрическая проницаемость линии.

Предложенная схема формирователя импульсов перенапряжения исследовалась нами на компьютерной модели в среде Multisim 11 [92, 93]. На рис 2.13 приведена исследуемая схема формирователя на разрядной линии, а на рис. 2.14 – результаты моделирования динамических характеристик формирователя. В качестве диода рассматривается Laser Components G-SPAD SAP500-Series [94].

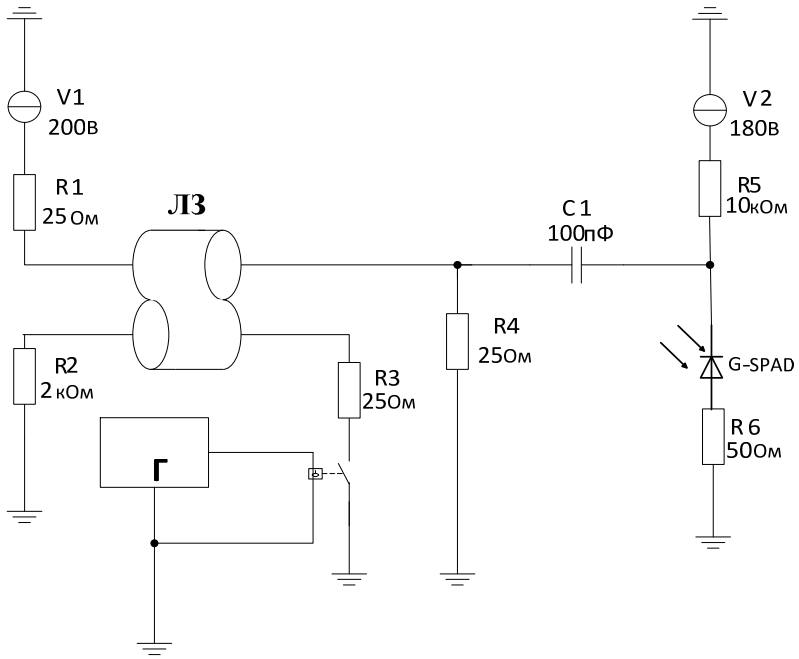


Рис. 2.13 - Схема формирователя импульсов перенапряжения с разрядной линией

Полученные данные показывают принципиальную возможность построения контроллера лавинного фотодиода, работающего в гейгеровском режиме, на основе формирователя импульсов перенапряжения с разрядной линией. Отличительной особенностью такого формирователя высокая стабильность длительности и амплитуды генерируемых стробирующих импульсов и простота регулировок этих параметров [95, 96].

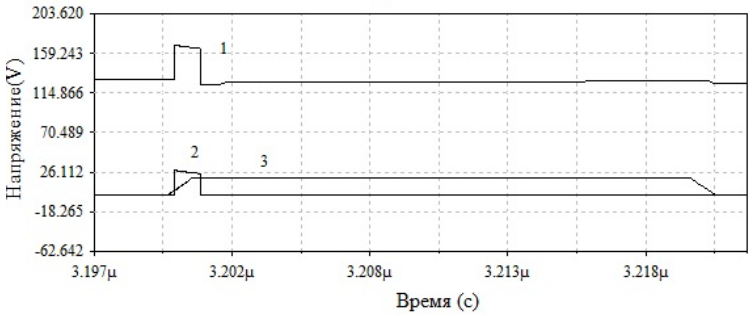


Рис. 2.14 - Результаты моделирования схемы формирователя стробирующего импульса, 1 – импульс на выходе формирователя, 2 – выходное напряжение G-SPAD, 3 – импульс запуска формирователя

2.6 Аппаратная платформа системы КРК

В качестве аппаратной платформы блоков приемного и передающего модулей (ПрОМ и ПОМ) мы рассматриваем соответствующие разработки наших партнеров [97], которые мы адаптируем для использования в разрабатываемой системе КРК – использование однофотонных импульсов и выставление специфического порога.

2.6.1 Усилительный контроллер лазерного диода

В качестве контроллера лазерного диода (ЛД) ADL65075TL в данной работе мы рассматривали использование микросхем ONET4201LD и ONET4211LD, разработанных фирмой Texas Instruments для построения оптоволоконных каналов связи с пропускной способностью вплоть до 4.25 Гбит/с. Характеристики микросхем взяты из datasheet [98], а их структурная схема приведена на рис. 2.15.

Микросхема в указанном диапазоне обеспечивает контроль излучением ЛД с активным сопротивлением ориентировочно равным 20 Ом. Резистор R_D на рис. 2.16 предназначен для гашения отражений управляющего сигнала от ЛД от выхода линии связи с ЛД. Номинал R_D определялся запасом мощности и внутренним сопротивлением лазерного диода, лежащим в пределах 4-7 Ом для лазеров с распределённой обратной связью или лазера с резонатором Фабри-Перо. В наших разработках планируется использование лазерного диода ADL65075TL.

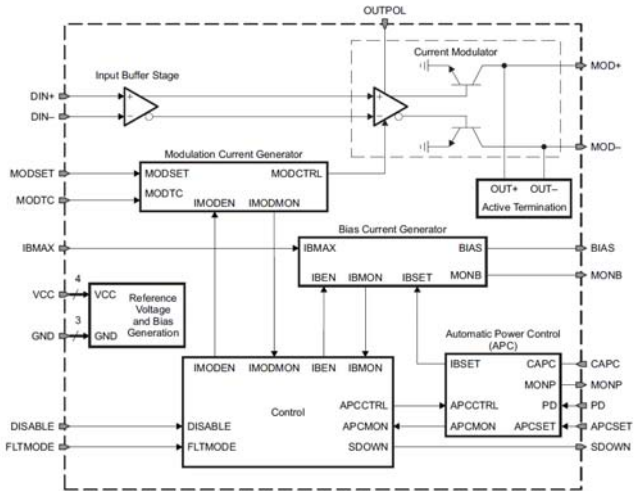


Рис. 2.15 – Структурная схема контроллера лазерного диода системы КРК

Контроллер ЛД на основе ONET4201LD был разработан, построен и исследован нашими партнерами из центра прикладных исследований полимерных оптических волокон по схеме рис. 2.16 [97]. Развязка управляющего сигнала и цепи питания ЛД на рис. 2.16 обеспечивается дросселем на основе ферритового кольца. Для демпфирования выбросов на фронтах управляющего сигнала лазерного диода используется RC цепь, состоящая из резистора R3 и конденсатора C3. Номиналы этих компонентов находятся экспериментальным путём.

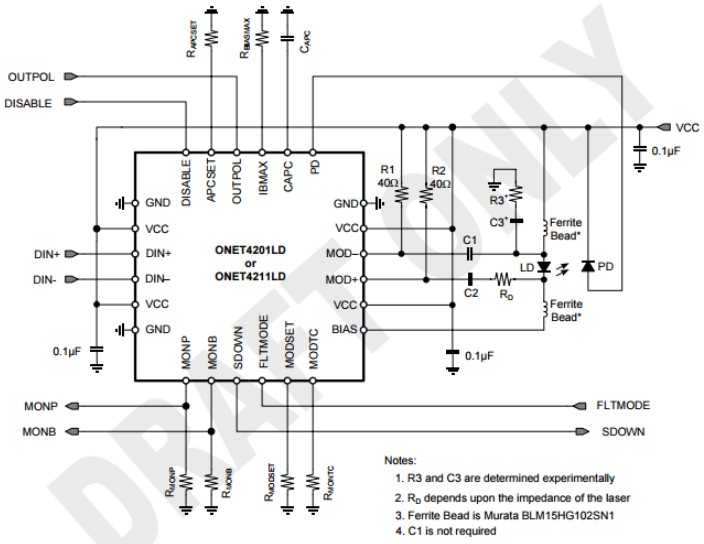


Рис. 2.16 – Принципиальная схема контроллера ЛД системы КРК на основе ONET4201LD

2.6.2 Усилительный тракт ПрОМ

Усилительный тракт ПрОМ обеспечивает усиление выходного сигнала высокочувствительного фотодиода (ФД) и включает в себя, малошумящий усилитель фототока ФД, предварительный линейный усилитель и усилитель-ограничитель.

Первый из названных каскадов обеспечивает преобразование сигнального фототока в аналоговое выходное напряжение. Нами рассматривался преобразователь по схеме рис. 2.17, построенной на основе микросхемы HFBR-25X6Z, включающей малошумящий трансимпедансный усилитель, объединенный с ФД в едином пластиковом корпусе [99]. Микросхема специально разработана для использования в скоростных волоконно-оптических каналах связи.

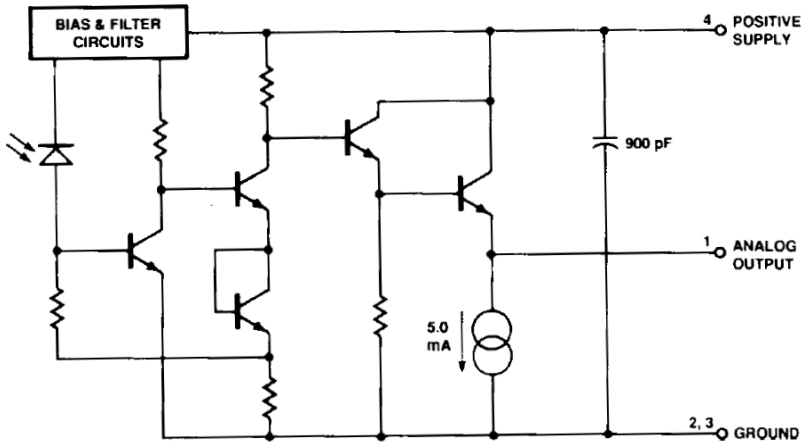


Рис. 2.17 – Функциональная схема преобразователя оптического сигнала микросхемы HFBR-25X6Z

Предварительный линейный усилитель ПрОМ мы планируем построить на основе той же микросхемы HFBR-25X6Z по принципиальной схеме рис. 2.18, разработанной и протестированной нашими партнерами из ПОВ-АС на основе HFBR-25X6Z [97].

В качестве усилителя – ограничителя (УУ) ПрОМ мы планируем применить микросхему фирмы Texas Instruments ONET4201PA [100]. Соответствующая структурная схема чипа представлена на рис. 2.19.

Микросхема обеспечивает усиление сигнала на 50 дБ, обеспечивает полностью симметричную амплитуду выходного сигнала для слабых входных сигналов величиной 3 мВ. в частотной полосе 155 Мбит/с – 4.25 Гбит/с. Широкий динамический диапазон УУ обеспечивает небольшое колебание задержки выходного сигнала даже при перегрузке УУ, при амплитуде входных сигналов до 1200 мВ.

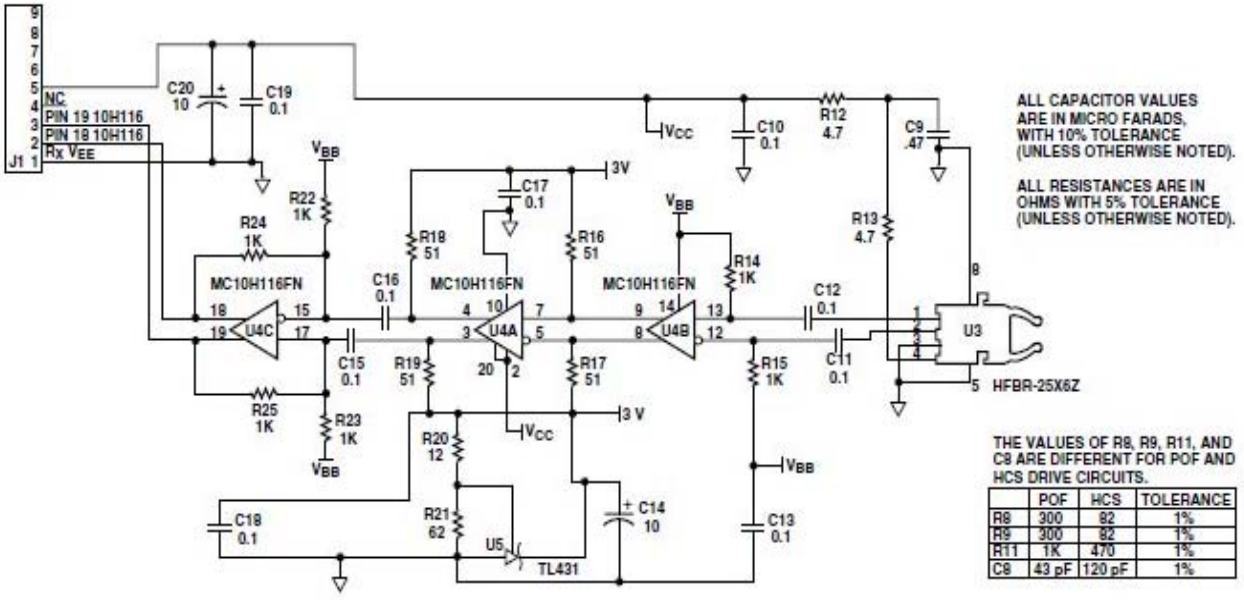


Рис. 2.18 – Принципиальная схема предварительного линейного усилителя ПрОМ на основе микросхемы HFBR-25X6Z

Структурная схема усилителя на рис. 2.19 включает скоростную линию передачи, регулируемый усилительный тракт, источник опорного напряжения и компаратор.

Высокочастотный сигнал на рис. 2.19 передаётся в усилительный тракт через входные порты DIN+/DIN-. Канал усиления УУ состоит из двухкаскадного линейного предварительного усилителя и трех каскадов основного усилителя, обеспечивающих уровень усиления порядка 50 дБ. Усиленный сигнал подаётся на выходные порт DOUT+/DOUT-.

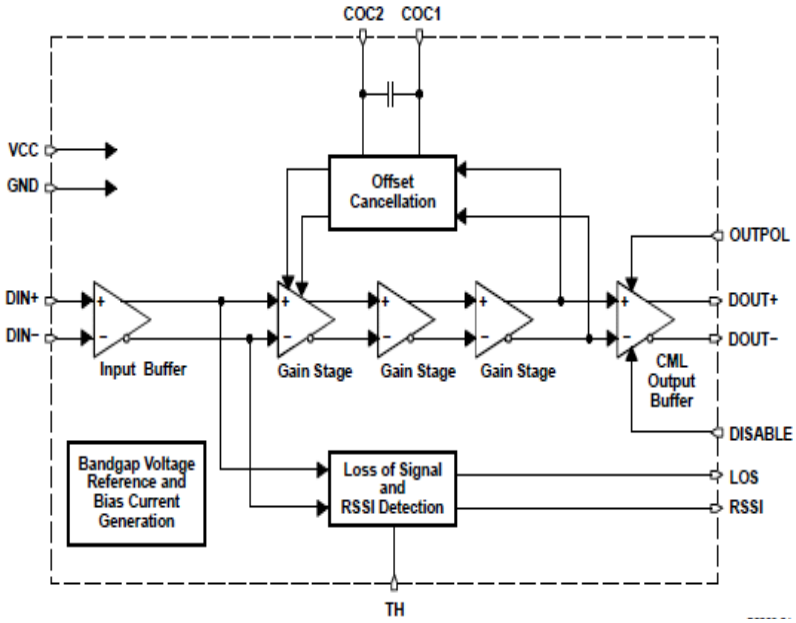


Рис. 2.19 Структура усилителя –ограничителя ПрОМ , построенного на основе ONET4201PA

2.7 Матричное описание трансформации квантовых состояний одиночных фотонов в последовательности разбалансированных интерферометров Маха-Цендера

Рассмотрим в начале одиночный однокубитовый вентиль, структурная схема которого представлена на рис. 2.20. Будем полагать, что вектор состояния квантовой частицы $|\psi_0\rangle$ на его входе представляет собой кубит, приготовленный в двумерном ортогональном вычислительном базисе, построенном на векторах $|0\rangle$, $|1\rangle$ (1.1).

Совместим каждый из базисных кет-векторов в (1.1) с одним из оптических портов ИМЦ. Состояние кубита $|\psi_4\rangle$ на выходных оптических портах ИМЦ, как видно из рисунка, будет определяться последовательным преобразованием (1.1) в квантовых вентилях Адамара, фазовращающем вентиле, а также вентиле временного сдвига. Обозначим унитарные операторы указанных логических устройств через **H, P** и **D** соответственно. Тогда преобразование кубита $|\psi_0\rangle$ в ИМЦ будет определяться уравнениями:

$$\left.\begin{aligned}
\left|\psi_1\right\rangle &= \mathbf{H}\left|\psi_0\right\rangle, \\
\left|\psi_2\right\rangle &= \mathbf{P}\left|\psi_1\right\rangle, \\
\left|\psi_3\right\rangle &= \mathbf{D}\left|\psi 2\right\rangle, \\
\left|\psi_4\right\rangle &= \mathbf{H}\left|\psi_3\right\rangle.
\end{aligned}\right\} \tag{2.11}$$

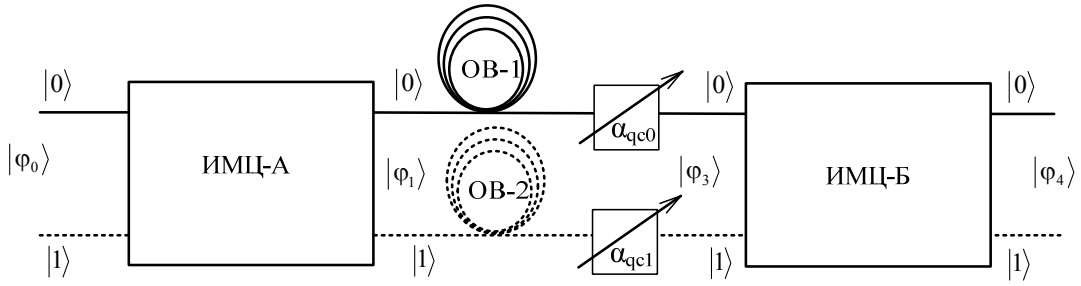


Рис. 2.21 Структурная схема разбалансированного интерферометра Маха-Цендера

Задача заключается в отыскании решения уравнений (2.11) и использование его для исследования трансформации $|\psi_0\rangle$ в системе из нескольких интерферометров, представленной на рис. 2.21.

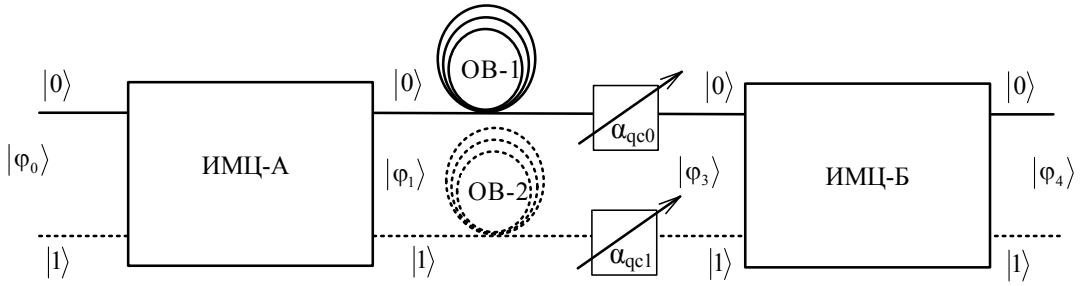


Рис. 2.22 Трансформация кубитов в системе из двух ИМЦ

2.7.1 Трансформация кубита в ИМЦ

Формальное решение системы линейных уравнений (2.11) дается как,

$$\left|\psi_4\right\rangle = \mathbf{H}\cdot\mathbf{P}\cdot\mathbf{D}\cdot\mathbf{H}\cdot\left|\psi_0\right\rangle. \tag{2.12}$$

Здесь и далее знак точки между операторами означает свертку матриц по соседним индексам. Далее необходимо задать матрицы **H**, **P** и **D** соответствующих унитарных операторов. Как уже отмечалось, матрица **H** волоконного сплиттера без потерь с коэффициентом деления оптического сигнала 50/50 совпадет с квантовым вентилем Адамара [13],

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.13}$$

Матрица **P** фазовращающего вентиля описывает фазовые сдвиги α_0 и α_1 оптического сигнала в плечах ИМЦ и может быть представлена в виде [2]:

$$\mathbf{P} = \begin{bmatrix} \exp(j\alpha_0) & 0 \\ 0 & \exp(j\alpha_1) \end{bmatrix} \tag{2.14}$$

Далее, следуя [1], введем линейный унитарный оператор временного сдвига **D**, описывающий относительный временной сдвиг одиночных фотонов в плечах интерферометра на время Δ. В дальнейшем будем полагать, что оператор **Dm**, определяющий соответствующий *m*-кратный временной сдвиг, выражается через **D** как:

$$\mathbf{Dm}=\mathbf{D}\cdot\mathbf{D}\ \mathbf{D}\ \ldots\ \mathbf{D}=\mathbf{D}^m.$$

Заметим, что при отсутствии сдвига (m=0) **Dm** представляется единичной матрицей.

С учетом сделанных замечаний матрицу **D** представим в виде:

$$\mathbf{D} = \begin{bmatrix} D & 0 \\ 0 & 1 \end{bmatrix} \tag{2.15}$$

Из соотношений (2.12)-(2.15) следует, что при $|\psi_0\rangle=|0\rangle$ вектор состояния кубита $|\psi_4\rangle$ на выходных портах $|0\rangle$ и $|1\rangle$ ИМЦ определится как:

$$|\psi_4\rangle = \frac{1}{2}\left[e^{j\alpha_0}D + e^{j\alpha_1}\right]|0\rangle + \frac{1}{2}\left[e^{j\alpha_0}D - e^{j\alpha_1}\right]|1\rangle \tag{2.16}$$

Формула (2.16) показывает, что состояние $|\psi_4\rangle$ одиночного фотона в портах $|0\rangle$ и $|1\rangle$ разбалансированного интерферометра представляется tb-кубитами, т.е. двумя разделенными промежутком времени Δ его возможными альтернативными состояниями.

Измерение данных временных кубитов осуществляется с помощью интерферометра Б, аналогичного ИМЦ-А, по схеме рис. 2.21. Формальную модель измерений можно получить путем замены в (2.12) состояния $|\psi_0\rangle=|0\rangle$ на входе ИМЦ на соотношение (2.16). При этом следует учесть, что матрицы **P**

фазовращающих вентилей интерферометров всегда различны. Эти различия в дальнейшем будем помечать нижними индексами фазовых переменных А и Б, например, как $\alpha_{А0}$ или $\alpha_{Б1}$. Кроме этого обозначим операторы сдвига интерферометров как $D_А$ и $D_Б$. При расчете кет-вектора $|\psi_4\rangle$ системы из двух ИМЦ следует также учесть фазовую матрицу $\mathbf{P}_{qc}$ квантового канала, в общем случае, состоящем из двух ОВ, объединяющих соответствующие порты интерферометров (см. рис. 2.22). Поэтому $\mathbf{P}_{qc}$ определим аналогично (2.14):

$$\mathbf{P}_{qc} = \begin{bmatrix} \exp\left(j\alpha_{qc0}\right) & 0 \\ 0 & \exp\left(j\alpha_{qc1}\right) \end{bmatrix}. \tag{2.17}$$

С учетом введенных обозначений, кубит $|\psi_4\rangle$ в портах $|0\rangle$ и $|1\rangle$ ИМЦ-Б определится как:

$$\left|\psi_4\right\rangle = \frac{1}{2}\mathbf{P}_{qc}\cdot\mathbf{H}_{Б}\cdot\mathbf{P}_{Б}\cdot\mathbf{D}\cdot\mathbf{H}_{Б}\cdot\begin{bmatrix} e^{j\alpha_{А0}}D_{А}+e^{j\alpha_{А1}} \\ e^{j\alpha_{А0}}D_{А}-e^{j\alpha_{А1}} \end{bmatrix}. \tag{2.18}$$

Воспользуемся соотношением (2.18) для анализа системы интерферометров, соединенных квантовым каналом, состоящим из одного оптического волокна. В данном случае один из диагональных членов матрицы (2.17) обращается в 0, поэтому из (2.18) следует,

$$\begin{aligned}\left|\psi_4\right\rangle = &\frac{1}{4}\left[\left(e^{j\alpha_{А1}}+D_{А}e^{j\alpha_{А0}}\right)\left(e^{j\alpha_{qc0}}e^{j\alpha_{Б1}}+D_{Б}e^{j\alpha_{Б0}}e^{j\alpha_{qc0}}\right)\right]|0\rangle - \\ -&\frac{1}{4}\left[\left(e^{j\alpha_{А1}}+D_{А}e^{j\alpha_{А0}}\right)\left(e^{j\alpha_{Б1}}e^{j\alpha_{qc1}}-D_{Б}e^{j\alpha_{Б0}}e^{j\alpha_{qc1}}\right)\right]|1\rangle\end{aligned} \tag{2.19}$$

Заметим, что операторы $D_А$ и $D_Б$ в (2.19) описывают сдвиги во времени наблюдаемой одиночного фотона при его распространении по длинным (Д) плечам ИМЦ-А, Б, а единичный оператор, $1=(D_А)^0=(D_Б)^0$ - отсутствие таких сдвигов для коротких (К) плеч интерферометров соответственно. Отсюда следует, что в рассматриваемом случае в каждом из портов $|0\rangle$ и $|1\rangle$ ИМЦ-Б состояние $|\psi_4\rangle$ представлено куквартами, кет-векторы которых имеют четыре допустимых динамических состояния. Одно из них в (2.19) представлено состоянием с нулевой задержкой (**Dm**=1), реализуемом на оптической траектории $К_А$-$К_Б$, еще два

состояния с однократной задержкой (**Dm**=$D_А$, $D_Б$), реализуемые на траекториях $Д_А$-$К_Б$ и $К_А$-$Д_Б$, а также одно состояние с двукратной задержкой (**Dm**=$D_А \cdot D_Б$) на траектории $Д_А$-$Д_Б$.

При идентичных конструкциях интерферометров, когда $D_А$=$D_Б$, слагаемые в круглых скобках оказываются вырожденными, т.е. соответствующие им состояния реализуются одновременно, размерность вектора состояний одиночного фотона на выходных портах второго ИМЦ снижается до 3, а сам объект $|\psi_4\rangle$ обращается в кутрит. Указанные линейно независимые динамические состояния кутрита выберем в качестве базисных векторов и обозначим как $|\alpha\rangle$, $|\beta\rangle$ и $|\gamma\rangle$. Тогда в соответствии с (2.19), проекции $|\psi_4\rangle$ на векторы $|0\rangle$ и $|1\rangle$ будут:

$$\langle i|\psi_4\rangle=\xi_{i\alpha}|\alpha\rangle+\xi_{i\beta}|\beta\rangle+\xi_{i\gamma}|\gamma\rangle, \qquad (2.20)$$

где i=0,1; $\xi_{i\alpha}$, $\xi_{i\beta}$, $\xi_{i\gamma}$ – комплексные амплитуды вероятности состояний $|\alpha\rangle$, $|\beta\rangle$ и $|\gamma\rangle$ кутрита в портах $|0\rangle$ и $|1\rangle$ соответственно.

Наиболее интересным информационным состоянием кутрита является состояние $|\beta\rangle$, формирующееся в условиях равенства оптических длин L_1 и L_2 траекторий $Д_А$-$К_Б$ и $К_А$-$Д_Б$, при которых квантовая частица способна интерферировать сама с собой [1, 2, 7, 8]. Результаты этой интерференции проявляются в зависимости амплитуд вероятности $\xi_{i\beta}$ состояний $|\beta\rangle$ в выходных оптических портах ИМЦ-Б от разности фаз $\phi=(\alpha_{Б0}+\alpha_{А1})-(\alpha_{Б1}+\alpha_{А0})$ и на практике используются для фазовых измерений комплексной амплитуды $\xi_{i\beta}$ [1, 2, 7, 8]. Действительно, из (2.19) видно, что при фазовом сдвиге ϕ оптического сигнала на отрезках L_1 и L_2 ИМЦ-А,Б амплитуды вероятностей состояния $|\beta\rangle$ в двух выходных портах ИМЦ-Б будут пропорциональны $\beta_1 \sim \cos(\phi/2)$, $\beta_2 \sim \sin(\phi/2)$ соответственно. Таким образом, вероятности регистрации одиночных фотонов в указанных точках ИМЦ-Б $P_1 \sim \cos^2(\phi/2)$ и $P_2 \sim \sin^2(\phi/2)$ зависят от настройки значения фазового сдвига ϕ фазовращающих вентилей ИМЦ-А,Б.

Недостатком рассмотренной схемы на рис. 2.22 детектирования tb- кубитов с одним ОВ является большие потери битрейта в квантовом канале связанные с

отбрасыванием направляемых в волоконный терминатор кубитов из порта $|1\rangle$ ИМЦ-А.

Снижение потерь можно получить в схеме рис. 2.22 с квантовым каналом, состоящим из двух оптических волокон. Отыщем $|\psi_4\rangle$ для такого канала. Воспользовавшись соотношениями (2.13-2.19) и по-прежнему полагая, что $D_{\text{А}}=D_{\text{Б}}$, получим,

$$\begin{aligned}|\psi_4\rangle=\frac{1}{4}\Big\{&\left(e^{j\alpha_{\text{А}1}}-D_{\text{А}}e^{j\alpha_{\text{А}0}}\right)\left(e^{j\alpha_{\text{Б}1}}e^{j\alpha_{qc0}}-D_{\text{А}}e^{j\alpha_{\text{Б}0}}e^{j\alpha_{qc0}}\right)+\\&+\left(e^{j\alpha_{\text{А}0}}+D_{\text{А}}e^{j\alpha_{\text{А}0}}\right)\left(e^{j\alpha_{\text{Б}1}}e^{j\alpha_{qc0}}+D_{\text{А}}e^{j\alpha_{\text{Б}0}}e^{j\alpha_{qc0}}\right)\Big\}|0\rangle-\\&-\frac{1}{4}\Big\{\left(e^{j\alpha_{\text{А}1}}-D_{\text{А}}e^{j\alpha_{\text{А}0}}\right)\left(e^{j\alpha_{\text{Б}1}}e^{j\alpha_{qc1}}+D_{\text{А}}e^{j\alpha_{\text{Б}0}}e^{j\alpha_{qc1}}\right)+\\&+\left(e^{j\alpha_{\text{А}1}}+D_{\text{А}}e^{j\alpha_{\text{А}0}}\right)\left(e^{j\alpha_{\text{Б}1}}e^{j\alpha_{qc1}}-D_{\text{А}}e^{j\alpha_{\text{Б}0}}e^{j\alpha_{qc1}}\right)\Big\}|1\rangle.\end{aligned}\qquad(2.21)$$

Из полученной формулы следует, что в канале, построенном из волокон с одинаковыми фазовыми характеристиками, когда $\alpha_{qc0}=\alpha_{qc1}$, амплитуда $\xi_{i\beta}$ состояния $|\beta\rangle$ кутрита в (2.20) обращается в ноль вследствие деструктивной интерференции фотона в обоих выходных портах ИМЦ-Б, прошедшего различные альтернативные траектории рассматриваемой схемы. Из (2.21) видно, что для состояний $|\alpha\rangle$ и $|\gamma\rangle$ указанная интерференция является конструктивной и приводит к двойному увеличению их амплитуд.

Структурой интерференционной картины в выходных портах можно, очевидно, управлять за счет изменения разности фаз $\phi=\alpha_{qc0}-\alpha_{qc1}$ в волокнах квантового канала. Так при $\phi=\pi$, согласно (2.21) условие конструктивной интерференции будет выполняться для состояния $|\beta\rangle$ кутрита, при этом состояния $|\alpha\rangle$ и $|\gamma\rangle$ окажутся подавленными [101].

2.7 Выводы ко второй главе

Предложена модель оценки помехоустойчивости ПрОМ на основе безразмерной дисперсии шумовых электронов и осуществление контроля параметров вероятности пропуска сигнала P_l и ложного сигнала P_f через варьирование уровня срабатывания порогового устройства. Предложена формула для расчета битовой скорости генерации ключа с учетом вероятности пропуска сигнала. Предложена формула для оценки вероятности ложного срабатывания ЛФД в гейгеровском режиме.

Расчетным путем доказана возможность реализации системы КРК с использованием в ПрОМ ЛФД S8664-05K в линейном режиме для заданных параметров. При $U_{\text{пор}}$ = 79 данный приемник способен обеспечить скорость генерации «сырого» ключа 10,2 Кб при вероятности ошибок P_f = 0,07.

Для Hamamatsu S8664-05K разработан импульсный источник питания по схеме повышающего преобразователя с выходным напряжением до 500 В и пульсациями, не превышающими 18 мВ.

Предложена функциональная схема формирователя импульсов перенапряжения с разрядной линией для высоковольтных диодов в гейгеровском режиме. В данной схеме предусмотрено активное гашение лавины. Приведены результаты симуляции в пакете Multisim для питания диода в гейгеровском режиме Laser Components G-SPAD SAP500-Series.

Адаптация предложения коллег по пороговому уровню ПрОМ, а также использование однофтонных посылок в аппаратной платформе для системы КРК. Усилительный контроллер лазерного диода, а также набор для усилительного тракта ПрОМ – микросхемы преобразователя оптического сигнала, предварительного линейного усилителя ПрОМ, усилителя-ограничителя ПрОМ.

Предложен матричный метод расчета структуры квантовых состояний одиночных фотонов в системе из двух разбалансированных ИМЦ, который легко обобщается на произвольное число интерферометров путем последовательного перемножения однотипных операторных матриц интерферометров и

соединяющих их квантовых каналов. При этом, как было показано, происходит динамическая стратификация состояния фотона в выходных портах интерферометра, превращая его в многоуровневую квантовую систему - кудит (q-dit).

3. ИССЛЕДОВАНИЕ СИСТЕМЫ КРК С ИСПОЛЬЗОВАНИЕМ ВРЕМЕННЫХ СДВИГОВ ОДНОУРОВНЕВЫХ СОСТОЯНИЙ ОДИНОЧНЫХ ФОТОНОВ

Данная глава посвящена решению четвертой из поставленных задач. Здесь описывается реализованная в программном пакете Simulink модель системы КРК с временным кодированием, работающей по протоколу С.Н.Молоткова 2004 г. (М04) [74], предложены и реализованы подсистемы статистического и интерферометрического контроля. Приведены результаты моделирования.

3.1 Модель системы КРК с временным кодированием

Рассмотрим разработанную в Simulink-Matlab [100, 103] модель системы КРК-ВК, структурная схема которой представлена на рис. 3.1.

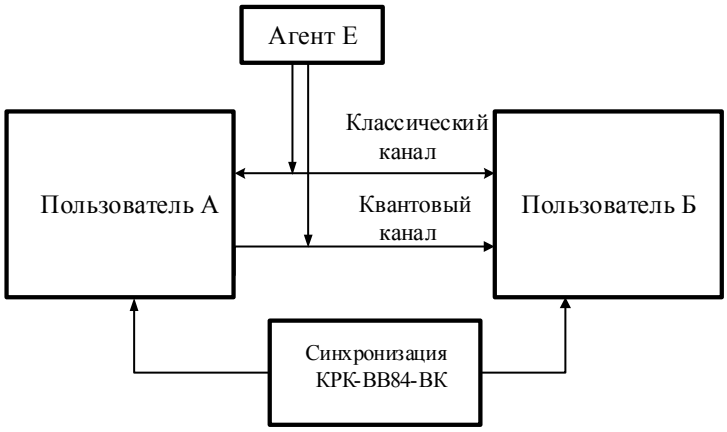


Рис. 3.1. Структурная схема КРК-ВВ-84-ВК

В программной модели используется несколько измененный протокол М04 [72]. Логическая схема протокола приведена на рис. 3.2. На нем изображен один тактовый интервал, в пределах которого показаны различные возможные кодовые состояния фотонов, далее в реализованной модели их роль будут выполнять короткие импульсы. Вертикальной жирной меткой на каждом рисунке обозначены тактовые синхроимпульсы. Символами Б-*i* слева на рис. 3.2 пронумерованы базисные состояния фотонов, а символами Δ_i снизу отмечены временные интервалы - тайм-слоты (ТС), используемые для кодирования состояния одиночных фотонов в пределах каждого из базисов. Введенные нами изменения

касались устранения дополнительных окон в базисе 1 для символа «0» и в базисе 3 для символа «1», а также замена значений символов в окнах базиса 3 на противоположные. Это было предпринято для обеспечения равной вероятности появления символов «0» и «1» в каждом ТС тактового интервала.

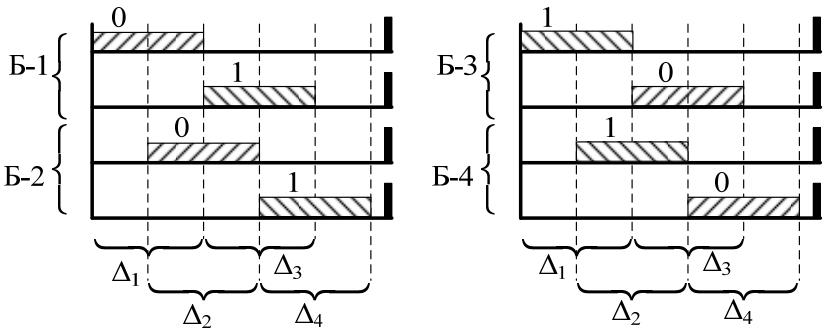


Рис. 3.2. Кодовые состояния базисов и окон протокола BB84-ВК

3.2 Структура приемо-передающей части системы КРК-ВК

Рассмотрим более подробно передающую часть, структурная схема которой дана на рис. 3.3. В соответствии с алгоритмом формирования секретного ключа, генераторами псевдослучайных последовательностей ПСП 0–1 и ПСП Δi задаются значения символов коротких импульсов и номер ТС Δ*i*. Для каждой пары сгенерированных чисел в дешифраторе кодовых состояний (КС) рассчитывается соответствующий номер временного базиса Б-*i* пользователя А. В зависимости от Δ*i* выбирается соответствующий тайм-слот в устройстве формирования ТС, в устройстве формирования импульсов при этом приготавливается короткий импульс, который имитирует фотон, затем с помощью блока AND происходит их логическое сложение. Далее полученная информационная посылка передается по квантовому каналу второму пользователю.

Приемная часть аппаратуры пользователя Б содержит узлы, идентичные вышеназванным. При этом генераторы ПСП 0-1 и ПСП Δ_i приемной стороны не синхронизированы с соответствующими генераторами передатчика, т.е. второй пользователь случайным образом выбирает ТС, в котором будет принимать короткий импульс. Если информационное сообщение детектировано в выбранном

окне, то пользователь Б пересылает пользователю А номер базиса. В случае когда на приемной стороне происходит совпадение Б-*i*, передающая сторона извещает об этом приемную и оба пользователя записывают значения символов из ПСП 0-1 в память как «сырой» ключ. Вышеописанные действия происходят в устройствах сравнения и записи.

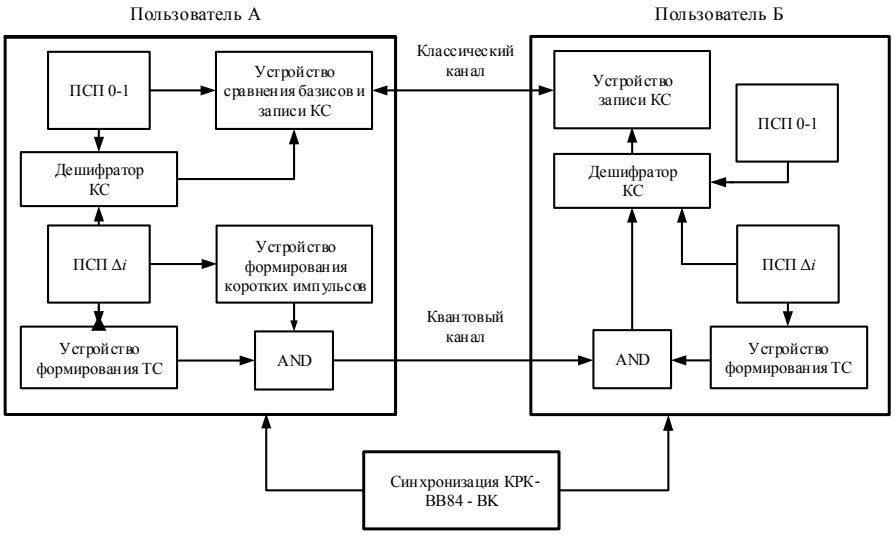


Рис. 3.3. Структурная схема передающей части системы КРК-ВК

Также стоит заметить, что для обеспечения конфиденциальности принятых коротких импульсов, сигнал о совпадении базисов передается пользователем Б не сразу, а в конце тактового интервала.

Рассмотрим реализацию каждого из блоков более подробно.

3.2.1 Устройство формирования ТС

Функциональная схема устройства формирования кодирующих временных интервалов – тайм-слотов (ТС) изображена на рис. 3.4. Каждый из четырех тайм-слотов генерируются на выходе логического оператора OR, ко входам которого подключены два блока Counter. Каждый из блоков Counter настроен на срабатывание после определенного количества пришедших на вход синхроимпульсов, при этом единичный сдвиг по времени происходит на длительность равную половине тайм-слота для корректной работы задержки сигнала в реальной системе.

Выбор необходимого временного окна происходит с помощью переключателя ТС, который является мультипортовым переключателем Multiport Switch. Он обеспечивает коммутацию одного из входных портов под действием управляющего сигнала, который формирует блок ПСП Δ_i. Результат работы устройства формирования ТС представлен на рис. 3.5.

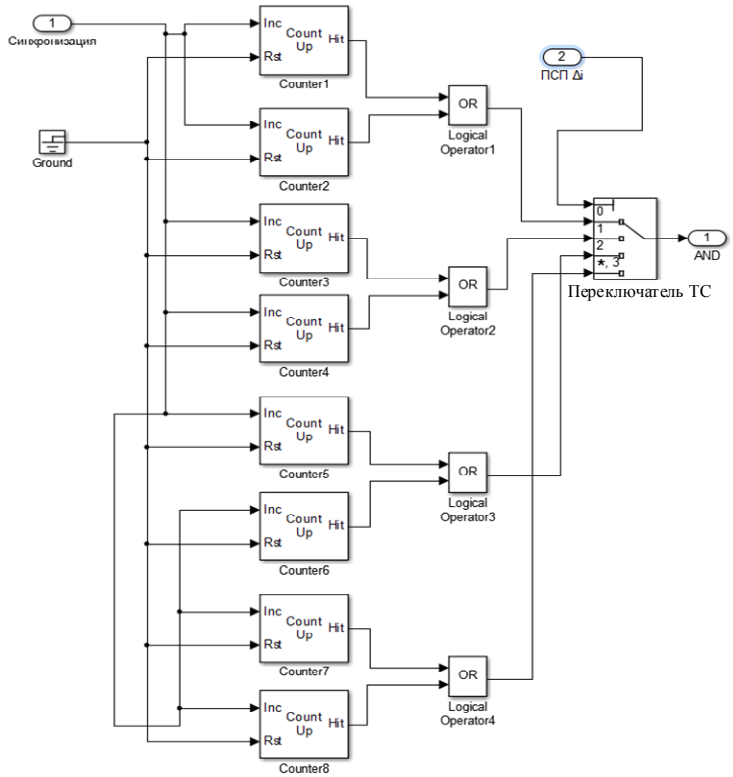
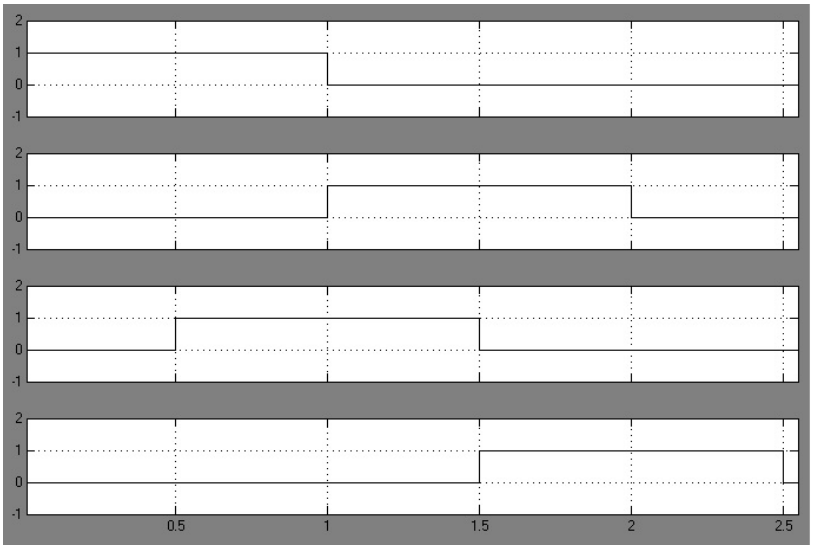


Рис. 3.4 Функциональная схема устройство формирование ТС



3.5 Сформированные ТС

3.2.2 Устройство формирования коротких импульсов

Функциональная схема устройства формирования коротких импульсов, имитирующих отклик ЛФД на одиночный фотон, представлена на рис. 3.6.

На выходе генератора коротких импульсов, которым является блок Pulse Generator формируются частая последовательность импульсов. С помощью счетчиков Counter 1-5 и Multiport Switch 1-4, тайм-слот делится на 5 частей,

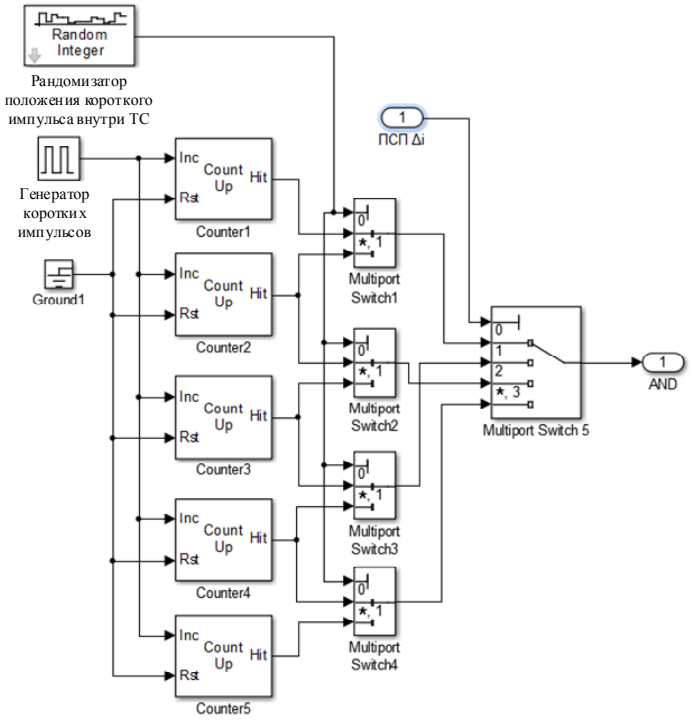


Рис. 3.6. Функциональная схема устройство формирования коротких импульсов

появление имитирующего фотон импульса возможно только в одной из них, выбор происходит случайным образом с помощью рандомизатора положения короткого импульса внутри ТС с помощью блока Random Integer Generator. Таким образом, реализуется дребезг импульса внутри ТС. С помощью Multiport Switch 5, управляемого блоком ПСП Δ_i, импульс формируется в выбранном тайм-слоте. Результат работы устройства формирования короткого импульса изображен на рис. 3.7.

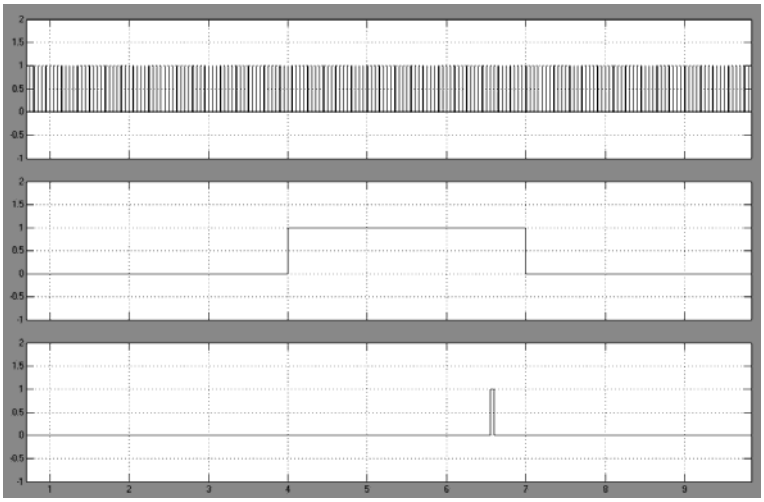


Рис. 3.7. Процесс работы устройства формирования состояния фотона, первая строка – последовательность с генератора коротких импульсов, вторая – управляющий импульс с рандомизатора положения короткого импульса внутри ТС, третья – полученный импульс.

3.2.3 Процедура имитации отклика ЛФД внутри тайм-слота

Результат работы устройства формирования короткого импульса, имитирующего отклик ЛФД внутри тайм-слота, устройства формирования ТС, а также результат их работы после прохождения через логический оператор AND (рис. 3.3) представлен на рис. 3.8.

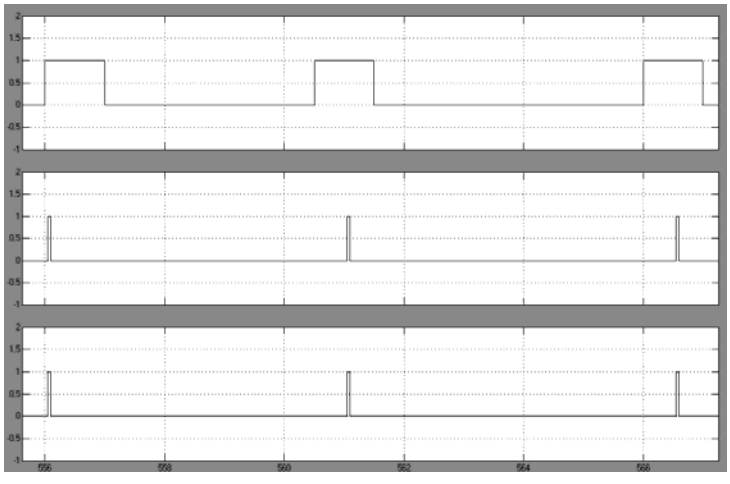


Рис. 3.8. Процесс формирования короткого импульса внутри ТС, первая строка – сформированные ТС, вторая – полученные импульсы, третья – полученная последовательность

3.2.4 Блоки ПСП 0-1 и ПСП Δ_i

Блоки ПСП 0-1 и ПСП Δ_i ПС реализованы на основе Random Integer Generator.

3.2.5 Дешифратор кодовых состояний

Дешифратор реализован блоком Look Up Table (2D), в строки Row заданы значения символов «1» и «0», а в столбцах Column - номера базисов Б-*i*, значения таблицы – номера тайм-слота Δ_i, рис. 3.9. Соответствия между этими параметрами составлены согласно используемому протоколу.

Breakpoints	Column	(1)	(2)	(3)	(4)
Row		***0***	***1***	***2***	***3***
(1)	***0***	1	3	2	4
(2)	***1***	3	1	4	2

Рис. 3.9. Таблица соответствий дешифратора

На рис. 3.10 представлен пример симуляция входных и выходных параметров дешифратора.

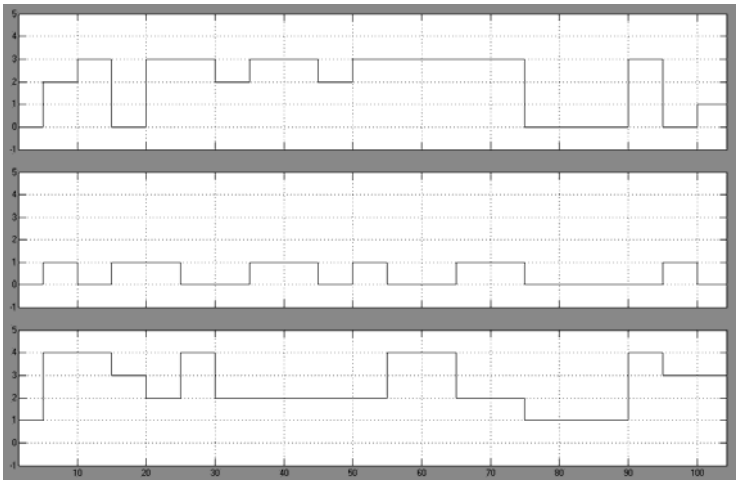


Рис. 3.10. Работа дешифратора, первая строка – входное значение номера тайм-слота Δ_i, вторая строка – входное значение символа 0-1, третья строка – выходное значение номера базиса Б-*i*.

3.2.6 Устройство сравнения базисов и записи кодовых состояний, устройство записи кодовых состояний

Функциональная схема устройства сравнения базисов и записи кодовых состояний представлена на рис. 3.11. Базисы ПА и ПБ сравниваются с помощью блока Relation Operator1, при совпадении выходным сигналом для него будет «1», иначе «0». При одинаковых номерах базисов, значение символа записывается в регистр памяти, реализованный блоком Triggered Write To Workspace, с помощью блока Clock также регистрируется время получения сообщения с номером базиса от ПБ. Факт совпадения базисов также передается пользователю Б. Записанная таким образом последовательность на обеих сторонах является «сырым» ключом.

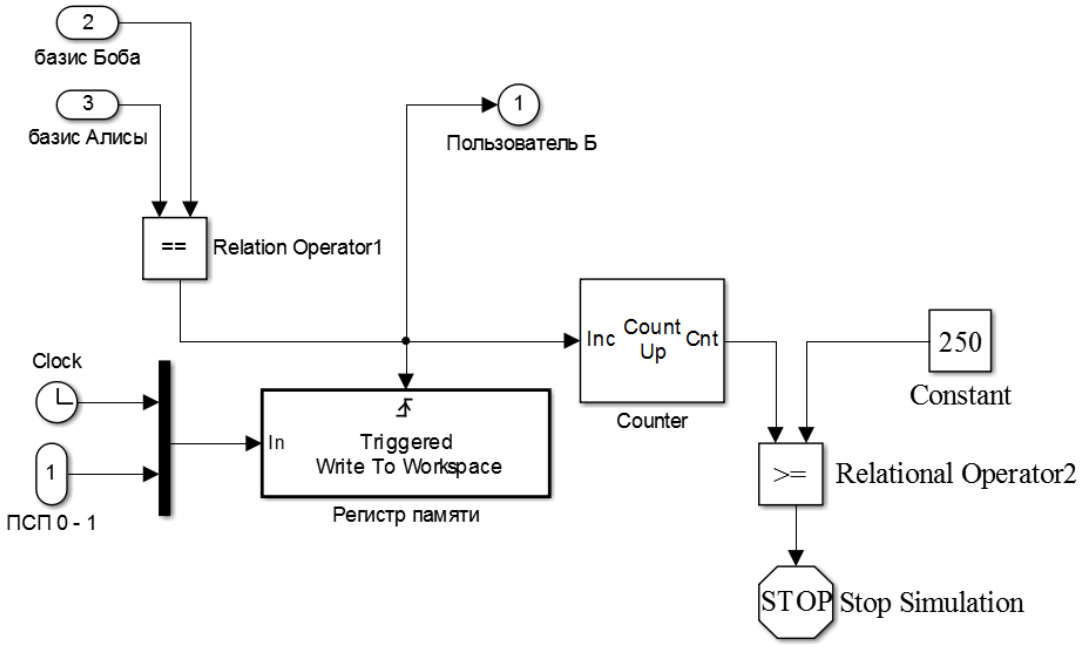


Рис. 3.11 Принципиальная схема устройства сравнения базисов и записи КС

Результат работы устройства сравнения и записи представлен на рис. 3.12.

Предусмотрена возможность остановки работы системы после достижения необходимой длины ключа. В блоке Constant выставляется количество символов, с помощью счетчика Counter фиксируется число совпадений. В блоке Relation Operator2 они сравниваются и в том случае если длина ключа превышает или

равно значению, выставленному в Constant, срабатывает блок Stop Simulation и останавливает общение между ПА и ПБ.

Устройство записи, которое расположено на стороне ПБ, имеет аналогичные блоки для записи значений совпавших базисов, а также возможность остановки работы системы после достижения необходимого количества символов [104]. Сформированный «сырой ключ» представлен на рис. 3.13.

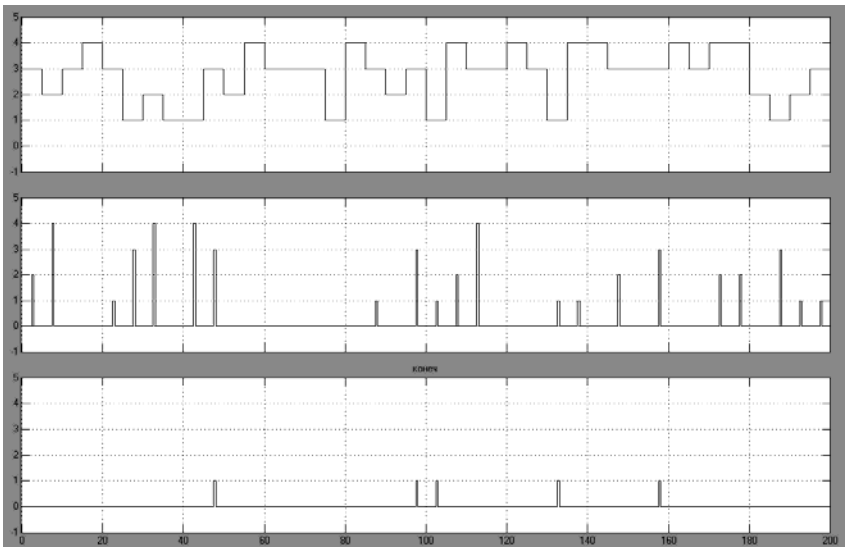


Рис. 3.12. Сравнение базисов ПА и ПБ, первая строка – номера базисов ПА, вторая строка – номера базисов ПБ, третья строка – единичные импульсы при совпадении.

3.3 Оценка шумов ПрОМ в модели системы

Разработанная модель использовалась для измерения вероятности генерации ложных символов P_f ключа, определяющей уровень ошибок системы, в отсутствии и при наличии белых гауссовых шумов ПрОМ, который реализован блоком Gaussian Noise Generator.

Обработка данных происходила с помощью подпрограммы. Она работает следующим образом: пользователь вводит с какого символа по какой необходимо сверить ключевую последовательность ПА и ПБ. Происходит проверка по соответствию количества символов у обоих пользователей. Далее происходит сверка символов, в случае, если ошибок нет, выдается соответствующее

сообщение, если же есть – выводятся порядковые номера тайм-слотов, в которых обнаружены ошибки (рис. 3.13).

Листинг данной программы:

```
g1=input(['s '],'s');
g2=input(['do '],'s');
h1=str2num(g1);
h2=str2num(g2);
I= Bob([h1:h2],[1,2]);
J= Alisa ([h1:h2],[1,2]);
if J (:,2) == I (:,2);
char 'Ошибок нет'
else
M1 = J (:,2) - I (:,2);
v1=[1:length(J)];
k1=v1';
x1=abs(M1);
S1=x1 .* k1;
H1=union(S1,S1,'rows');
H2=H1+(h1-1);
H2(1,:)=[]
End.
```

Проведенные эксперименты показали, что ошибочные символы в массивах $\mathbf{m}_А$ и $\mathbf{m}_Б$ возникают лишь при наличии шумов в системе. Усредненных по 10 выборкам расчетные зависимости P_f от уровней шума системы и порога U_0 компаратора ПрОМ, реализованного блоком Compare to Constant, нормированного к средней амплитуде a отклика приемника на состояния фотонов, показаны на рис. 3.14. Цифрами *1* и *2* на рис. 3.14 отмечены кривые $P_f(U_p)$, измеренные при различных среднеквадратичных амплитудах шумового напряжения $U_ш$ на входе компаратора ПрОМ, нормированного относительно a. В первом случае $U_ш = 0{,}15$,

а во втором, $U_{ш} = 0{,}45$. Из представленных графиков хорошо видна возможность удержания допустимого системных ошибок на уровне ~11% [64] с помощью регулировки порога ПрОМ U_p.

Alisa <25x2 double>

	1	2	3
1	37.5000	0	
2	47.5000	1	
3	62.5000	0	
4	82.5000	0	
5	92.5000	1	
6	147.5000	1	
7	217.5000	1	
8	227.5000	0	
9	247.5000	0	
10	262.5000	0	
11	282.5000	1	
12	307.5000	0	
13	357.5000	0	
14	412.5000	1	
15	432.5000	1	
16	477.5000	1	
17	542.5000	0	
18	587.5000	0	
19	682.5000	0	
20	702.5000	0	
21	757.5000	1	
22	777.5000	1	
23	902.5000	0	
24	912.5000	0	
25	967.5000	1	
26			

Bob <25x2 double>

	1	2	3
1	37.5000	0	
2	47.5000	1	
3	62.5000	0	
4	82.5000	0	
5	92.5000	1	
6	147.5000	1	
7	217.5000	1	
8	227.5000	0	
9	247.5000	0	
10	262.5000	0	
11	282.5000	1	
12	307.5000	0	
13	357.5000	0	
14	412.5000	1	
15	432.5000	1	
16	477.5000	1	
17	542.5000	0	
18	587.5000	0	
19	682.5000	0	
20	702.5000	0	
21	757.5000	1	
22	777.5000	1	
23	902.5000	0	
24	912.5000	0	
25	967.5000	1	
26			

Рис. 3.13 Записанные в регистр памяти значения символов с указанием времени на стороне ПА (слева) и ПБ (справа)

Следует заметить, что повышение U_0 хотя и способствует снижению ошибок P_f, но одновременно, с вероятностью P_l, приводят к пропускам сигнальных посылок в моменты опроса пороговой схемы и снижению скорости B генерации массива КП (2.1).

Зависящие от $U_{ш}$, U_p, $p(1)$, k_p параметры B, P_f, вместе со статистическим распределением состояний фотонов $p(n)$, являются основными системными показателями. Динамическое изменение этих параметров может указывать на возможные попытки взлома ключа, поэтому их непрерывный мониторинг является одной из задач блока контроля статистики системы рис. 3.2. Измерение

средней скорости приема состояний фотона B и распределения $p(n)$ при этом проводится путем непосредственных измерений состояний фотона на приемной стороне квантового канала. Следует заметить, что для контроля $p(n)$ пригодны фотодиоды, работающие в линейном режиме, чувствительность которых, ограниченная флуктуацией коэффициента умножения M, темновым током и др., может обеспечивать режим счета одиночных фотонов [87].

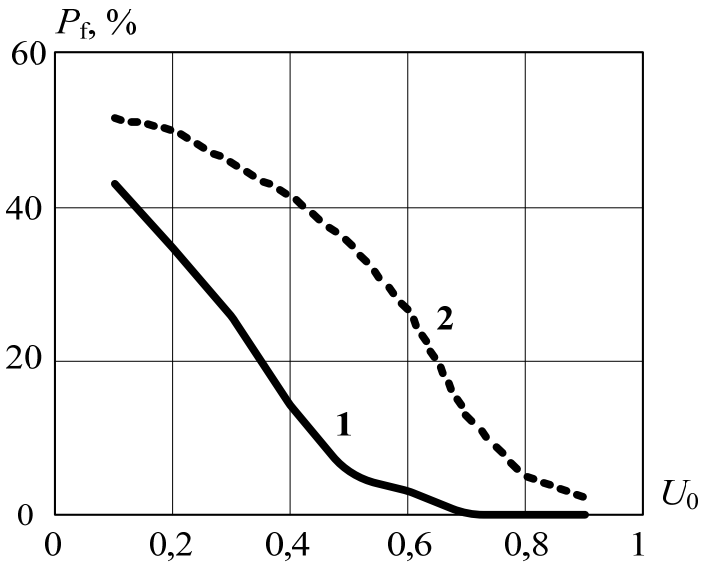


Рис. 3.14 Доля ложных символов в зависимости от порога компаратора ПрОМ

Уровень же ошибок P_f оценивается пользователями путем периодического обмена частью ключей $\mathbf{m}_A$ и $\mathbf{m}_Б$ по классическому каналу [104, 105].

3.4 Статистическая обработка сигналов в системах КРК

Формулы (2.1)-(2.7) позволяют рассчитать двумерную зависимость $B(P_f, \alpha_0 L)$. Пример расчета такой поверхности дан на рис. 3.15. Здесь шаг изменений аргументов по оси αL составляет 2.5 дБ, а по оси P_f - 3%. График получен для m=0.1 и ПрОМ, рассчитанного на работу с ЛФД S8664-05K в линейном режиме с коэффициентом лавинного размножения 100 и темновым током $0.15*10^{-9}$ А.

С помощью $B(P_f, \alpha_0 L)$ можно установить безопасные для конкретных видов атак агента Е границы значений скорости генерации КП B и длины квантового канала L [106].

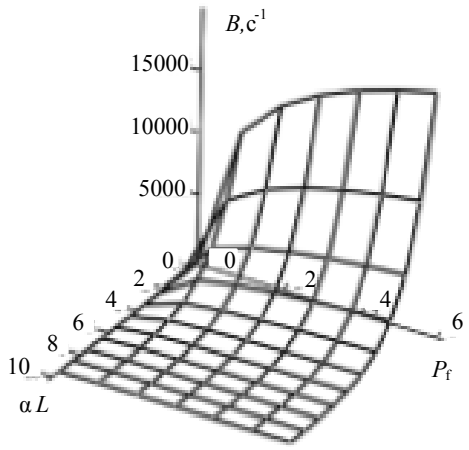


Рис. 3.15 Зависимость скорости генерации ключа от P_f
и ослабления в канале связи

3.4.1 Подсистема статистического контроля

Для усиления защищенности рассмотренного выше протокола КРК с временным кодированием предлагается использовать подсистему статистического контроля. Рассмотрим ее логическую структуру. Известно, что в условиях приготовления на передающей стороне квантового канала когерентных состояний одиночных фотонов их среднее число m в импульсе выбирается равным 0,1 [7]. Таким образом, только 10% переданных пользователем А сообщений содержат хотя бы один фотон, а 90% будут пустыми. В случае, если в канале связи присутствует нелегитимный пользователь, пытаясь замаскировать перехват данных, он пересылает приемной стороне свою последовательность, стараясь повторить полученную им от ПА. Так как генерация фотонов в определенном временном интервале носит вероятностный характер, АЕ вносит изменения в распределение вероятностей появления пустых, одно-, двух- и более фотонных посылок, что регистрируется ПБ.

Перехватывая данные, АЕ может действовать двояко. С одной стороны, она может пытаться отправлять информационные посылки пользователю Б в каждом перехваченном от пользователя А сообщении, т.е. сохранять значение в 10% посылок, которые содержат хотя бы одну квантовую частицу. В этом случае АЕ

необходимо будет существенно увеличить среднее значение относительно стандартного для того, чтобы исключить передачу Б пустых посылок относительно перехваченных ею и не допустить снижение битовой скорости генерации секретного ключа *B*. Рассмотрим это более подробно.

При работе системы без АЕ среднее числа фотонов составляет 0,1 соотношение согласно пуассоновскому распределению $p(1) \sim 0{,}09$, а вероятность двух- и более фотонных посылок будет составлять ~ 0,006, т.е. первых будет значительно больше, чем вторых. Однако в случае увеличения среднего значения, например, до 3, когда вероятность появления пустых сообщений будет незначительной, $p(0) \sim 0{,}05$, $p(1) \sim 0{,}15$, а все остальные, которых будет большинство ~ 0,8 будут содержать два и больше фотона. Таким образом, без вмешательства Е в квантовый канал связи доля однофотонных посылок будет выше, чем двух- и более фотонных. В случае же перехвата и использования Евой достаточно большого значения среднего числа частиц в сообщении, ситуация будет обратная – однофотонных посылок будет меньше, чем двух- и более фотонных. Таким образом, с помощью отслеживания количества фотонов в принятом Б сообщении можно сделать вывод о наличии перехвата данных в канале связи.

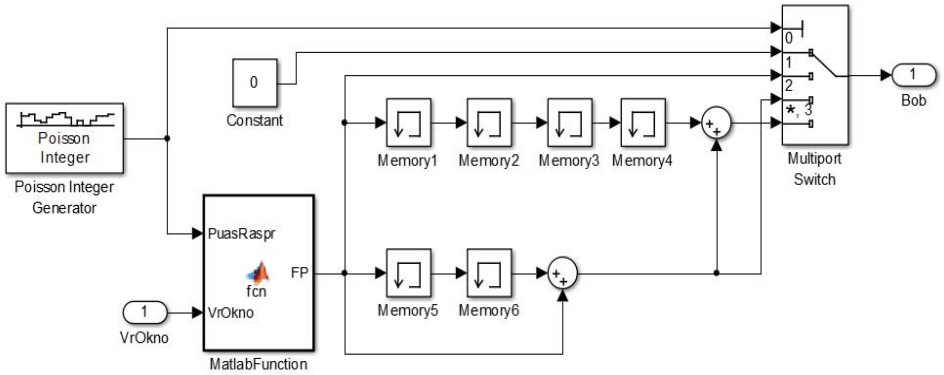


Рис. 3.16. Реализация пуассоновского распределения импульсов на стороне ПА

В другом случае, агент Е может пытаться обеспечить среднее число фотонов равным 0,1 при передачи своих информационных посылок, однако тогда существенно возрастет количество пустых сообщений относительно принятых от

А и значительно снизится другой контролируемый легитимными пользователями показатель - скорость *B,* что также будет детектировано.

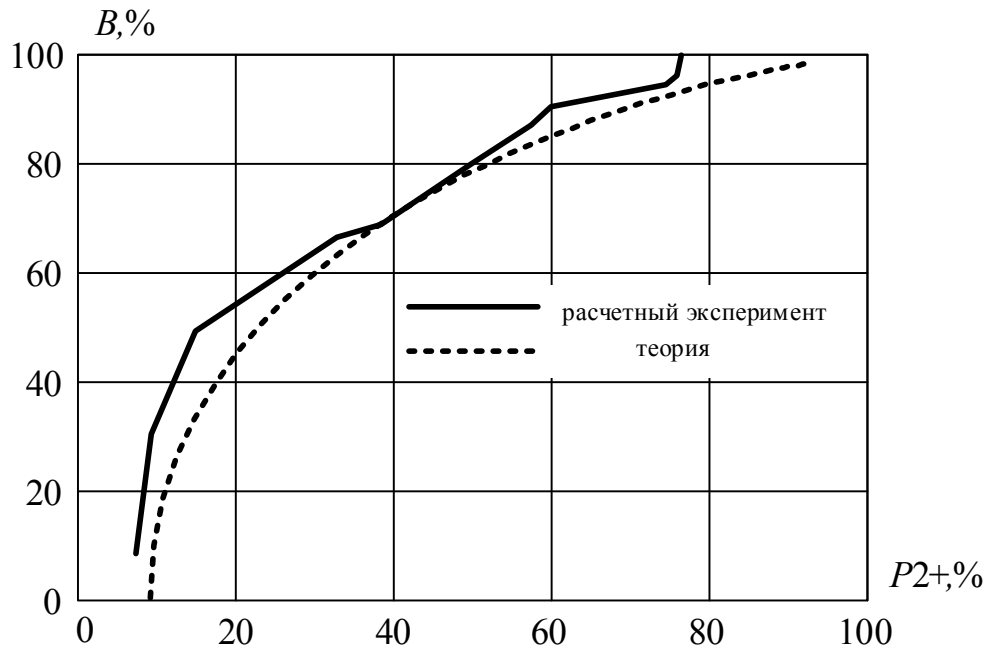


Рис. 3.17 Теоретическая и экспериментальная зависимости изменения битовой скорости *B* от процентной доли двух- и более фотонных посылок в условиях присутствия нелегитимного пользователя в квантовом канале

В разработанной нами программе присутствует возможность моделировать подобную атаку АЕ, а также соответствующее изменение распределения вероятности *p*(n). Модель подсистемы, включающая в себя устройство для приготовления КС с пуассоновской статистикой представлена на рис. 3.16. Здесь в блоке Poisson integer generator, в котором устанавливается необходимое среднее значение, подается управляющий сигнал на Multiport Switch, на выходе которого формируется соответствующее количество импульсов – ноль, один, два или три. Данные импульсы в заданном временном окне, которое определяется случайно выбранным базисом, передаются на сторону Б.

Аналогичным устройством, предназначенным для имитации заданного среднего числа фотонов в квантовом канале в ходе атаки, снабжена и сторона Е. Подсчет статистики *p*(n) происходит с помощью подпрограммы статистического контроля на стороне Б.

Результаты исследования программной модели в присутствии E представлены на рис. 3.17. Здесь приведены графики расчетного эксперимента и теоретической зависимости битовой скорости генерации ключа, нормированные относительно максимальной битовой скорости генерации ключа в возмущенном AE квантовом канале, от процентного состава двух- и более фотонных квантовых состояний $|\alpha_i\rangle$ в последовательности фотонов, передаваемых по квантовому каналу.

Из приведенного графика видно, что реализация AE алгоритмов построения клон-машины, связанных либо с сохранением битрейта кубитов в квантовом канале, либо сохранением стандартного пуассоновского распределения $p(n)$ числа фотонов n в состояниях $|\alpha\rangle$ приводит к ~9-кратному увеличению доли многофотонных состояний в последовательности $|\alpha_i\rangle$, или к ~10-кратному снижению квантового битрейта. Динамическое измерение указанных параметров и лежит в основе построения подсистемы статистического контроля системы КРК.

Таким образом, моделирования активности AE в квантовом канале системы КРК, выполненная в разработанной нами программной модели, совпала с ожидаемым результатом. Отсюда следует, что контроль средней битовой скорости B, а также относительного числа многофотонных квантовых состояний в принятых сообщениях позволяет выявить наличие атаки E на квантовый канал системы вне зависимости от среднего числа m [107].

3.5 Интерферометрический контроль

Описанная выше процедура статистического контроля трафика в квантовом канале не может обеспечить безусловной защищенности канала КРК. Например, применение подсистемы статистического контроля оказывается не эффективным в случае использования нелегитимным пользователем клон-машины на основе не глауберовских, а фоковских состояний $|n\rangle$ со заданным числом n квантовых частиц. В качестве способа преодоления указанного системного недостатка в работе рассмотрена возможность дополнения базовой модели системы КРК,

построенной на протоколах M04 - DB04, подсистемой интерферометрического контроля.

Как основу построения указанной подсистемы мы рассматривали известную технологию случайной вставки в последовательность состояний $|\psi_n\rangle$ квантовых частиц в квантовом канале особых контрольных кубитов $|\psi^*\rangle$, так называемых состояний-ловушек (decoy-states или DS-кубитов), позиция которых во фрейме $|\psi_k\rangle$ затем раскрывается легитимными пользователями в ходе протокольных переговоров по классическому каналу (DS-протокол КРК). В качестве $|\psi^*\rangle$ мы рассматривали возможность использования tb-кубитов, приготавливаемых из классического когерентного состояния $|\psi\rangle$ с помощью ИМЦ-А и детектируемых в ИМЦ-Б. При этом обеспечивается случайная вставка $|\psi^*\rangle$ в общую последовательность $|\psi_k\rangle$ и непрерывный контроль $|\psi_n\rangle$ на предмет содержания DS-кубитов, а физически контролируемым показателем состояний $|\psi_n\rangle$ в ИМЦ-Б является видность интерференционной картины амплитуд вероятностей КЧ. Указанный алгоритм исключает возможность регулярной и корректной вставки клон-машиной нелегитимным пользователем случайных DS-кубитов $|\psi^*\rangle$ в последовательность $|\psi_n\rangle$.

Подобная структура интерференционного контроля состояний $|\psi^*\rangle$ в системе КРК рассматривалась ранее в работах других авторов [75, 76]. При этом в квантовом канале на входе приемника пользователя Б поток $|\psi_i\rangle$ разделяется на две равные части. Одна из них регистрировалась ПрОМ-2 и использовалась для организации подсистемы интерферометрического контроля, а другая, с выхода ПрОМ-1, – для формирования последовательностей $\mathbf{k}_{АБ}$. Указанное прореживание потока снижает основной показатель системы - скорость генерации ключевой последовательности $\mathbf{k}_{АБ}$. Предложенная нами схема подсистемы интерферометрического контроля для оптоволоконной КРК-BB84-M04 - DB04, основанная на использовании tb-кубитов в качестве decoy-states $|\psi^*\rangle$, свободна от указанного недостатка [108, 109].

3.5.1 Оценка необходимого числа измерений для детектирования нелегитимного пользователя

Показателем, характеризующим эффективность подсистемы интерферометрического контроля, может служить среднее время детектирования работы КМ в квантовом канале $T_д$. Для рассмотренного выше DS-протокола значение $T_д$ можно выразить через число N тактовых интервалов во фрейме, а также число измерений $N_д$, необходимое для реализации указанного метода детектирования как:

$$T_д = \zeta(\alpha L, M, U_{пор}) \cdot N_д \cdot N/(N^* \cdot B_0) \quad (3.1)$$

где $\zeta(\alpha L, M, U_{пор}) = B_0/B$ - определяемый выражением (2.1) скалярный коэффициент, зависящий от ослабления αL оптического сигнала в квантовом канале, порога срабатывания $U_{пор}$ компаратора фотоприемника и связанных с ним вероятностей пропуска и генерации ложного сигнала, учитывающий снижение битрейта в системе. Параметр $N_д$ в (3.1) определяет число измерений, необходимых для фиксации с заданной доверительной вероятностью 1-β интерференционной картины, а N^* - число DS-вставок во фрейме.

Из приведенной формулы видно, что интервал $T_д$ сокращается с увеличением числа тактовых интервалов фрейма, занятых проверочными символами.

Для отыскания $N_д$ в (3.1) учтем, что в приближении нормального закона распределения точность интервальной оценки Δn совокупности из n-измерений, т.е. отклонения среднего и истинного значения измерения не более чем на Δn, с доверительной вероятностью 1-β выражается через t-распределение $t_{\alpha n}$ и погрешность измерений δn [110]. Полагая, что в рассматриваемом случае $\delta n = P_f$, получим выражение для Δn [110]:

$$\triangle n = t_{\beta_n - 1} \frac{\delta n}{\sqrt{n}} \quad (3.2)$$

На рис. 3.18 приведен график зависимости $\Delta n(t_{0.95,n\text{-}1})$, рассчитанный по формуле (3.2) для уровня P_f=0,11 и доверительной вероятности 0.95. При расчете распределения Стьюдента число степеней свободы полагалось равным n-1. Из

приведенных данных следует, что точность Δn мало изменяется при $n>4$. По этой причине уровень $N_д$ целесообразно установить равным 4. В таком случае из формулы (3.1) следует, что при $B_0 \approx 10^6$, $\zeta \approx 2 \cdot 10^{-3}$, $N=1024$ и $N^*=1$ реализация DS-протокола в системе КРК-ВК с использованием работающих при комнатной температуре фотоприемников позволяет обеспечить время детектирования $T_д \approx 1{,}8$ с. Как видно из (3.1), повысить скорость детектирования можно, например, за счет увеличения числа проверочных символов N^*. Однако в рамках DS-протокола такой прем одновременно приведет к пропорциональному снижению битрейта B.

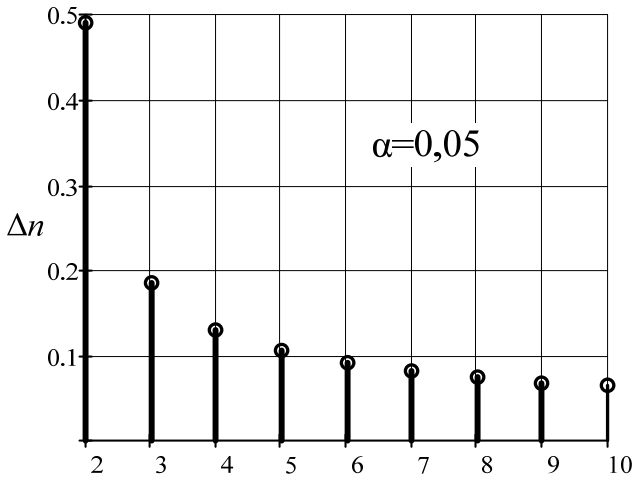


Рис. 3.18 Зависимость точности интервальной оценки Δn от числа измерений n при доверительной вероятности 0.95

Радикального увеличения скорости детектирования $(T_д)^{-1}$ можно достичь при протокольной организации, позволяющей проведение интерференционного контроля в каждом тактовом интервале фрейма без снижения B, при котором отношение N/N^* в формуле (3.1) обращается в единицу.

3.6 Программная модель для симуляции работы подсистемы интерферометрического контроля

В данном параграфе представлена реализация схемы, рассмотренной в этой главе модели системы КРК (рис. 3.19)

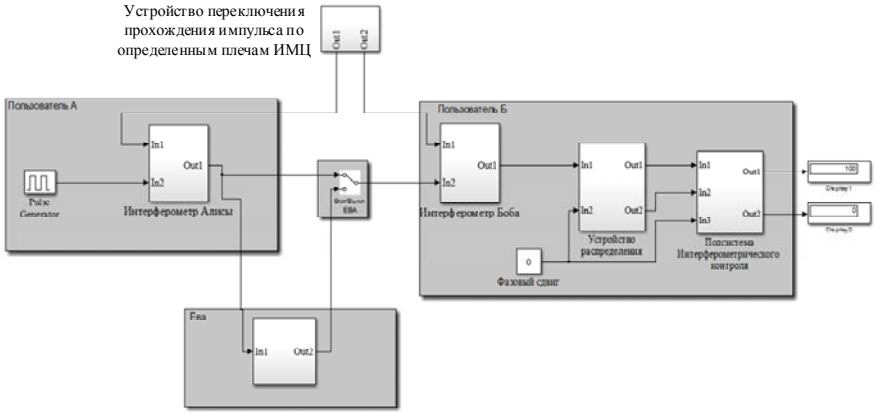


Рис. 3.19 Функциональная схема реализации интерферометрического контроля для модели системы КРК

3.6.1 Устройство переключения прохождения импульса по определенным плечам ИМЦ

Случайный выбор прохождения короткого импульса по определенному пути ИМЦ (рис. 3.20) работает следующим образом: к легитимным пользователям А и Б передается кодовая комбинация, которая состоит из 0, 1 и 2. При этом распределение вероятностей следующее, для 0 и 1 – по 25%, для прохождения по короткому-короткому и длинному-длинному пути; для 2 – 50%, для прохождения по короткому-длинному и длинному-короткому пути ИМЦ-А и ИМБ-Б.

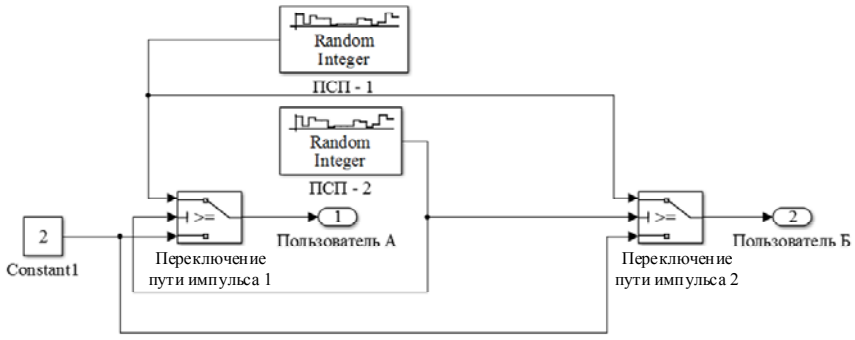


Рис. 3.20 Устройство переключения прохождения импульса по определенным плечам ИМЦ

Блоки ПСП - 1, 2, реализованные на основе Random Integer, выдают случайные последовательности 0 и 1. В блоках Switch, названных Переключение пути фотона 1 и 2, происходит сравнение пришедшего на средний вход с блока ПСП - 2

значения с 0,5, которое установлено в настройках блока Switch. В том случае, если с ПСП подается меньшее значение, то пользователю будет отправлена 2, с блока Constant1, иначе значение, пришедшее с ПСП - 1 для Пользователя А и Б.

3.6.2 Устройство имитации ИМЦ-А, ИМЦ-Б

На рис. 3.21 представлено устройство имитации ИМЦ-А. Управляющий импульс с устройства переключения прохождения прохождения импульса по определенным плечам ИМЦ идет к программному блоку имитации пути импульса, при этом в зависимости от пришедшего символа выбирается тот или иной путь с определенной задержкой, которые реализованы блоками Transoprt delay и названы Задержка 1 и 2, с зависимостью для прохождения по разным плечам ИМЦ, изложенной в предыдущем параграфе. С помощью блока переключения пути импульса, выполненного на основе Multiport Switch,

происходит выбор имитации прохождения по необходимому плечу.

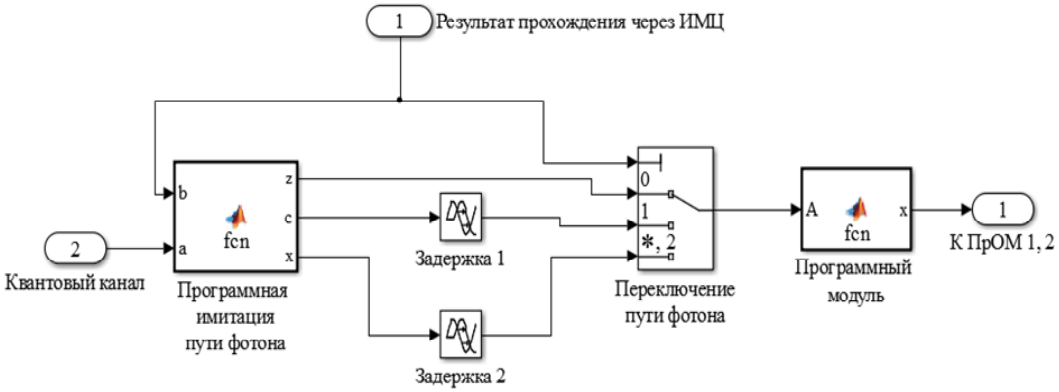


Рис. 3.21 Функциональная схема ИМЦ

Устройство имитации ИМЦ-Б полностью аналогично.

3.6.3 Устройство распределения коротких импульсов на один из ПрОМ

Схема устройства распределения представлена на рис. 3.22. Программный модуль выполнен с помощью блока Matlab Function. Его основная задача, в зависимости от заданного фазового сдвига распределять фотоны на один из ПрОМ.

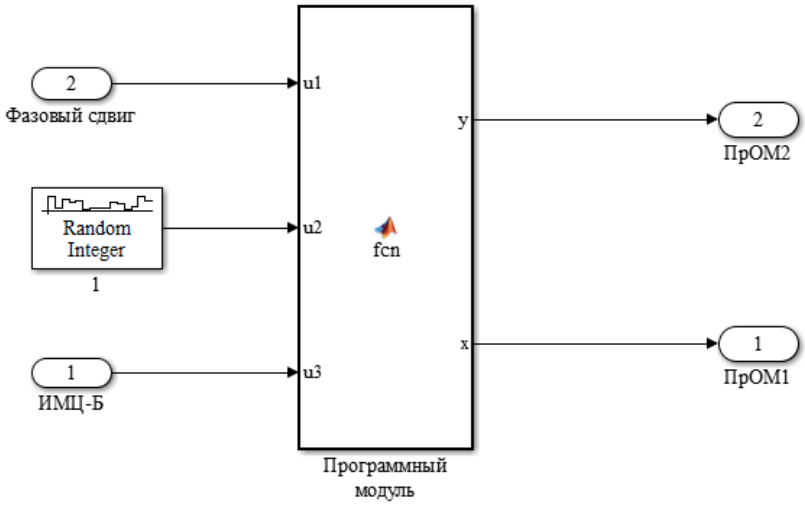


Рис. 3.22 Функциональная схема устройства распределения коротких импульсов

3.6.4 Подсистема интерферометрического контроля

Схема подсистемы интерферометрического контроля представлена на рис. 3.23.

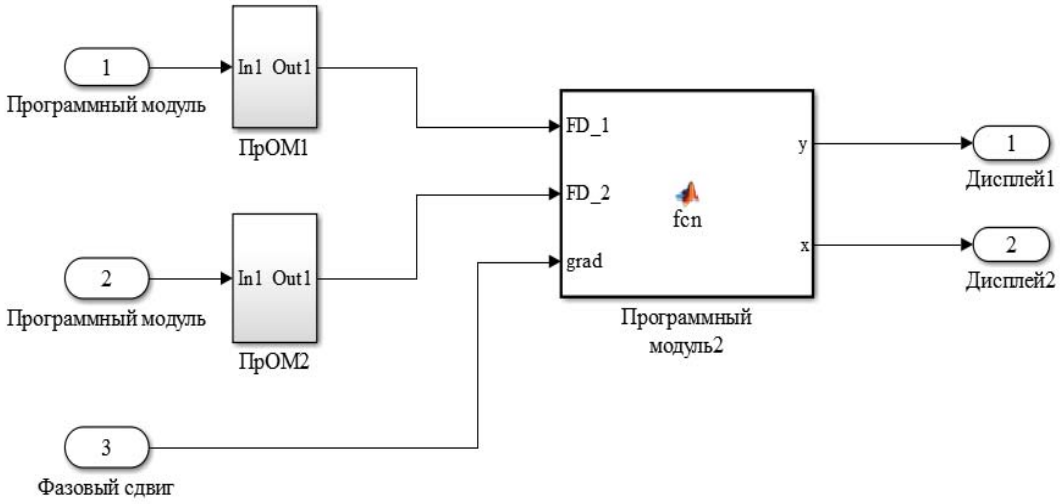


Рис. 3.23 Функциональная схема подсистемы интерферометрического контроля

В данной схеме ПрОМ1 и ПрОМ2 включают в себя в счетчики, результат с них проходит к программному модулю 2. В нем происходит подсчет срабатываний каждого из ПрОМ и их процентное соотношение, которое выводится на дисплеи для каждого из них.

3.6.5 Результаты моделирования работы интерферометрического контроля

Рассмотрим результаты моделирования работы интерферометрического контроля в присутствии и отсутствии АЕ.

Для первого случая, когда такого присутствия нет, результаты даны на рис. 3.24. Доля срабатываний первого n_{fd1} и второго n_{fd2} ПрОМ меняются в зависимости от установленного фазового сдвига от 0 до 100%.

В условиях, когда в квантовом канале присутствует нелегитимный пользователь, перехватывающий сообщения, срабатывания того или иного ПрОМ не зависят от фазового сдвига. На рис. 3.25 изображены доля срабатываний ПрОМ-1 в присутствии n_{fd1E} и отсутствии n_{fd1} АЕ в зависимости от фазового сдвига Δϕ.

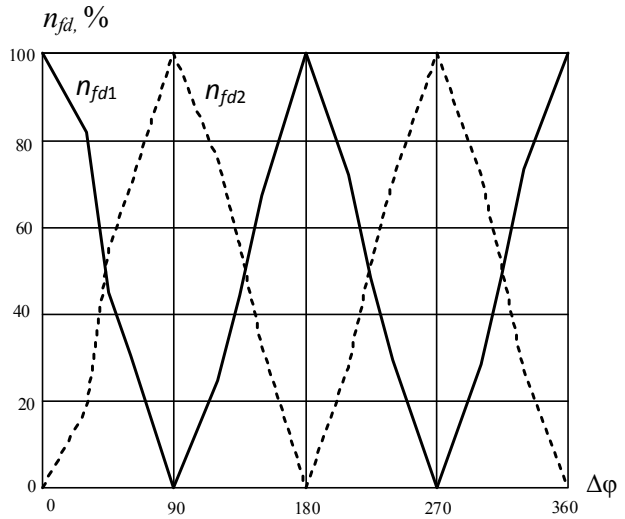


Рис. 3.24 Доля срабатываний ПрОМ-1, 2 в зависимости от фазового сдвига Δφ

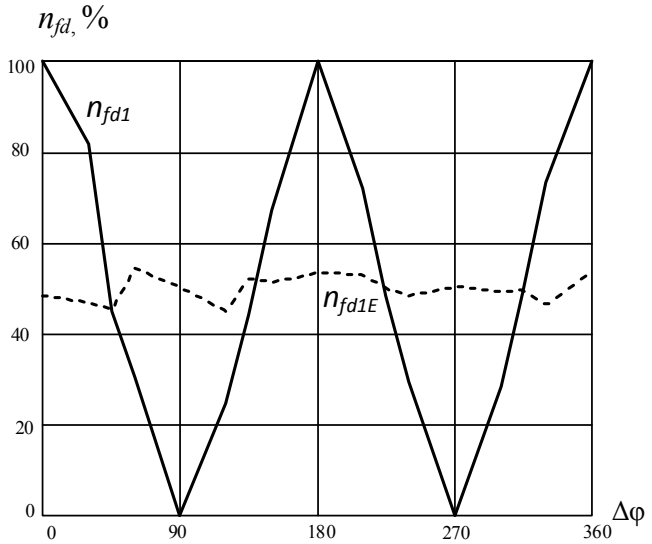


Рис. 3.25 Доля срабатываний ПрОМ-1 в присутствии и отсутствии АЕ

3.7 Выводы к третьей главе.

К основным результатам главы можно отнести следующие.

По алгоритму Молоткова С.Н. разработана и реализована программная модель системы КРК с ВК на базе протокола BB84. С помощью разработанной модели проведены расчетные эксперименты по исследованию влияния внутренних шумов ПрОМ. Получены зависимости P_f при различных среднеквадратичных амплитудах шумового напряжение $U_ш = 0{,}15$ и $U_ш = 0{,}45$ в зависимости от порога компаратора ПрОМ, значения которых нормированы относительно средней амплитуды отлика приемника. Из полученных результатов сделан вывод о возможности удержания допустимого для работы протокола BB84 уровня P_f.

В качестве мер дополнительной защиты системы предложены подсистемы статистического и интерферометрического контроля.

В программной модели реализована возможность учета статистики появления пустых, однофотонных, а также двух- и более фотонных посылок. Построена зависимость увеличения битовой скорости B до стандартного значения от вероятности появления двух- и более фотонных посылок при внедрении АЕ в канал связи и использования ею разных средних значений количества фотонов в каждой посылке согласно пуассоновской статистике. Сделан вывод о необходимости контроля системных показателей B и вероятности появления двух- и более фотонных $p(2+)$ посылок для детектирования возможного перехвата данных.

Реализована программная модель интерферометрического контроля, а также необходимые блоки для работы данной подсистемы, проверки ее работоспособности. Проведены соответствующие результаты расчетных экспериментов по детектированию присутствия нелегитимного пользователя в квантовом канале.

Показана общая функциональность системы, а также ее повышение защищенности с помощью подсистем статистического и интерферометрического контроля.

4. СИСТЕМА КРК-ВК НА ОСНОВЕ НЕОРТОГОНАЛЬНЫХ tb - КУБИТОВ

В данной главе рассматривается предложенный метод временного кодирования временных tb-кубитов, описывается логический и физический уровни.

4.1 Система КРК с временными сдвигами tb-кубитов

Проблема повышения защищенности протокола КРК с временным кодированием однофотонных состояний может быть решена не только за счет применения мер защиты, рассмотренных в главе 3, но также и за счет применения двухуровневых tb-кубитов. В данной параграфе будет рассмотрены несколько уровней системы КРК, работающей по данному принципу.

4.1.1 Логический уровень системы КРК с временными сдвигами tb-кубитов

Логический уровень рассматриваемой здесь системы КРК, в основном, является адаптацией описанного выше протокола ВВ-84 с поляризационным кодированием к работе с tb- кубитами, однако содержит ряд специфических особенностей. Одна из особенностей связана с формированием двух не ортогональных базисов, используемых стороной ПА в каждом такте последовательности $\mathbf{m}_A$. С этой целью нами, аналогично [32, 33], образовано два временных ортогональных базиса **I** и **II**, составленные из ортогональных пар кет-векторов состояний tb- кубита. Именно,

$$\text{базис } \mathbf{I}\text{: } |\psi_{02}\rangle,|\psi_{22}\rangle; \tag{4.1а}$$

$$\text{базис } \mathbf{II}\text{:, } |\psi_{32}\rangle,|\psi_{12}\rangle. \tag{4.1б}$$

Все базисные векторы в (3) приготавливаются из основного состояния одиночного фотона $|\psi_0\rangle$ на выходе ИМЦ-А за счет 1, 2, или 3-х кратного сдвига динамической переменной с указанным вектором:

$$|\psi_3\rangle=\mathbf{D}|\psi_2\rangle=\mathbf{D}|\psi_1\rangle=\mathbf{D}|\psi_0\rangle, \tag{4.2}$$

где **D -** оператор сдвига на время Δ [1].

Соотношение между базисными векторами $|\psi_m\rangle$ (m=0,1,2,3) поясняется рисунком 4.1. Стрелкой → на рис. 4.1 помечено соответствие между $|\psi_m\rangle$ и двоичными кодовыми символами 0 и 1.

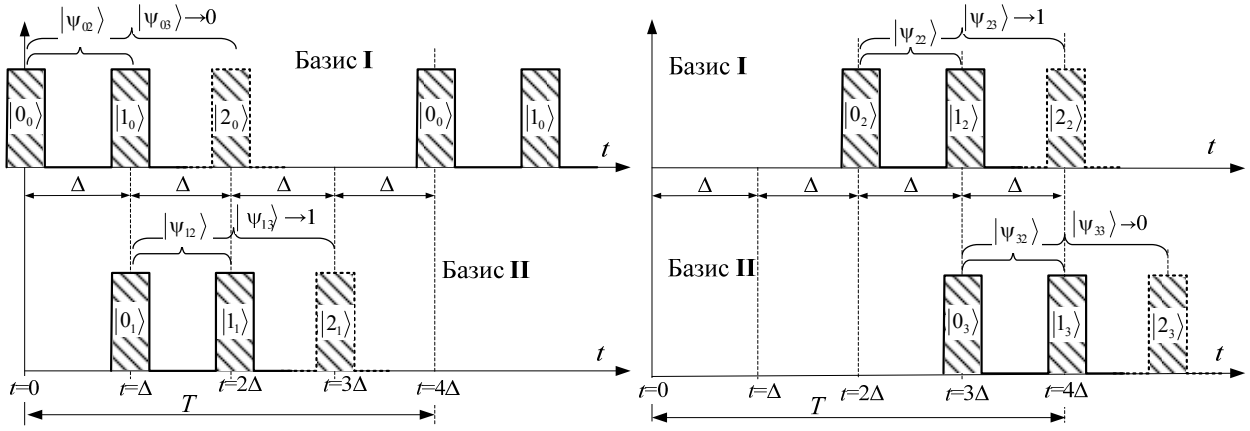


Рис. 4.1 Связь четырех сдвинутых во времени состояний tb- кубитов $|\psi m2\rangle$ и кутритов $|\psi m3\rangle$ с базисами I и II и кодовыми символами 0 и 1 на тактовом интервале

Заштрихованными областями на тактовом интервале выделены тайм слоты, т.е. временные области в окрестности t=0, Δ, 2Δ и 3Δ, в пределах которых на стороне ПБ возможна локализация квантовой частицы. В формулах (1.1) и (2.20) эти области описываются кет-векторами $|0\rangle$, $|1\rangle$ и $|2\rangle$. Связь данных векторов с введенными выше базисными векторами $|\psi_m\rangle$ для 2-х или 3-х уровневых состояний определим аналогично (2.20),

$$|\psi_{mn}\rangle=\alpha|0_m\rangle+\beta|1_m\rangle+\gamma|2_m\rangle. \qquad (4.3)$$

Здесь первый индекс (m=0, 1, 2, 3) в обозначении $|\psi_{mn}\rangle$ указывает на номер базисного кета, а второй – определяет число его состояний (n=2,3). В рассматриваемой здесь схеме КРК в квантовом канале пользователем А приготавливаются только двухуровневые (n=2) состояния фотонов (time-bin qubits), поэтому $|\psi_{m2}\rangle$ в (4.3) представляется лишь первой парой векторов $|0_m\rangle$ и $|1_m\rangle$. Кутрит и связанный с ними третий уровень $|2\rangle$ (на рис. 4.1 выделен

пунктирной линией) в (4.3) формируются лишь после обработки tb-кубитов $|\psi_{m2}\rangle$ в интерферометре на приемной стороне Б (см. рис. 4.2). Важно отметить, что кутрит $|\psi_{m3}\rangle$ в плечах ИМЦ-Б представлен двумя состояниями, обозначенными на рисунке 4.2 как $|\psi_{m3,1}\rangle$ и $|\psi_{m3,2}\rangle$. Их амплитуды определяют вероятности регистрации частиц в соответствующих плечах интерферометра.

Из рисунка 4.1 видно, что в рассматриваемой системе однозначная связь $|\psi_{m3}\rangle$ с переносимым им двоичным символом имеет место лишь для второго члена суммы (4.3), кет-вектора $|1_m\rangle$, локализованного в (m+1) тайм-слоте тактового интервала. В данной связи, на этапе согласования базисов состояния $|0_m\rangle$ и $|2_m\rangle$ принятых стороной Б кутритов $|\psi_{m3,1}\rangle$ и $|\psi_{m3,2}\rangle$ не должны приниматься в расчет.

Выше отмечалось, что в сбалансированных ИМЦ-А,Б именно $|1_m\rangle$ является наиболее информационным состоянием кутрита $|\psi_{m3}\rangle$. Оно характеризуется тем, что амплитуды вероятности β в (4.3) в ~1,42 раза превышает значения амплитуд α и γ. Еще более важным является проявление в данном состоянии интерференции амплитуд вероятностей кубитов, определяющей отмеченную ранее зависимость вероятности регистрации одиночных фотонов в плечах ИМЦ-Б от фазового сдвига ϕ фазовращающих вентилей ИМЦ-А, Б. Эта зависимость позволяет сторонам А и Б контролировать амплитуды вероятностей состояний $|\psi_{m31}\rangle$ и $|\psi_{m32}\rangle$, и связанную с ними целостность кубитов $|\psi_{m2}\rangle$ при их передаче по квантовому каналу [108].

Другая важная особенность рассматриваемой системы КРК заключается в том, что кубиты $|\psi_{m2}\rangle$ на стороне А всегда приготавливаются в суперпозиции состояний $\alpha = \beta = \sqrt{0.5}$. Последнее означает равную вероятность появление в квантовом канале фотона в состояниях $|0_m\rangle$ и $|1_m\rangle$, или, другими словами, равную вероятность локализации кубита $|\psi_{m2}\rangle$ в двух тактовых тайм слотах: m-м и m+1-м (рис. 4.1). Отсюда, с учетом данных рис. 4.1, можно заключить, что в рассматриваемой схеме КРК, как и при классическом поляризационном кодировании, ортогональные базисы **I** и **II,** в которых приготавливается последовательность $\mathbf{m}_A$, развернуты друг относительно друга на 45 градусов. В данных условиях попытки

клонирования $\mathbf{m}_A$ стороной АЕ (рис. 4.2) будут всегда связаны с необходимостью принятия ею решений о том, в каком базисе был приготовлен каждый кубит случайной последовательности $\mathbf{m}_A$. Уровень неизбежных при этом ошибок всегда контролируется сторонами А и Б в рамках стандартных протокольных переговоров по классическому каналу. Таким образом, присутствие и вынужденная активность АЕ в квантовом канале устанавливается по генерации АЕ избыточных ошибок в выборе базиса.

Следует отметить, что основной объем информации об указанных ошибках содержится в обычно не используемых сведениях о состояниях кутритов $|\psi_{m3}\rangle$ в тактах последовательности $\mathbf{m}_A$, где состояния базисов ПА и ПБ не совпали. Эти сведения обычно отбрасываются при формировании всей ключевой последовательность $\mathbf{k}_{АБ}$ [7, 15]. Особенностью обсуждаемого здесь протокола КРК является обязательное включение в обмен сторонами А и Б указанной не конфиденциальной информацией по скоростному классическому каналу, очевидно, усиливающего его защищенность.

Выделим еще один аспект, связанный с преобразованием кубитов $|\psi_{m2}\rangle$ в состояния $|\psi_{m3}\rangle$. Выше отмечалось, что при штатном преобразовании такого рода векторы $|0_m\rangle$, $|1_m\rangle$ и $|2_m\rangle$ кутрита могут регистрироваться в m-м, m+1-м и m+2-м тайм-слотах тактового интервала с вероятностями соответственно: 0.25, 0.5 и 0.25. В силу указанной выше неопределенности, подмена кубита $|\psi_{m2}\rangle$ в квантовом канале неизбежно приведет к изменению статистического распределения одиночных фотонов по тактовому интервалу. Можно показать, что в случае такой подмены $|\psi_{m2}\rangle$ регистрации фотонов возможны в (m-1)-м, m-м, (m+1)-м, (m+2)-м и (m+3)-м тайм-слотах с относительными вероятностями ~ 0.083, 0.25, 0.33, 0.25 и 0.083 соответственно. Контроль указанной статистики позволяет дополнительно усилить защищенности системы.

4.1.2 Физический уровень системы КРК

Аппаратная реализация рассматриваемой системы КРК, структурная схема которой приведена на рисунке 4.2, предполагает использование относительно простой элементной базы [7, 32, 33].

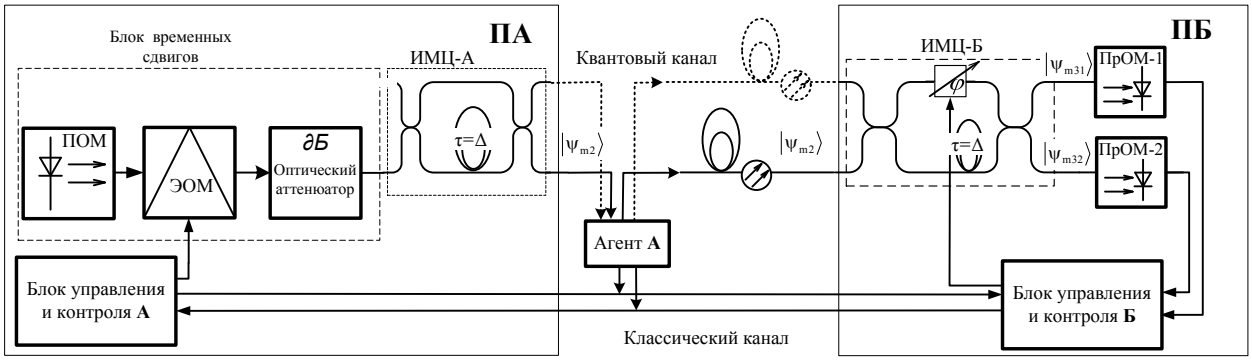


Рис. 4.2 Функциональная схема аппаратной части системы КРК с временными сдвигами tb- кубитов

Формирование одиночного фотона в базовом состоянии $|\psi_0\rangle$ в этой схеме происходит путем стробирования лазерного излучения передающего оптического модуля (ПОМ) электрооптическим модулятором (ЭОМ) и дальнейшего его ослабления в оптическом аттенюаторе. Локализация состояния $|\psi_0\rangle$ в нужном тайм-слоте тактового интервала, в соответствии с кодовыми состоянием $|\psi_{m2}\rangle$ по рис. 4.1, обеспечивается соответствующим временным сдвигом управляющего сигнала ЭОМ на время τ=0, Δ, 2Δ или 3 Δ. tb- кубиты приготавливаются из $|\psi_0\rangle$ в расположенном далее ИМЦ-А. Сформированная таким образом последовательность $\mathbf{m}_A$ с выхода интерферометра направляется в ОВ квантового канала. В интерферометре ИМЦ-Б временные кубиты $\mathbf{m}_A$ преобразуется в две последовательности кутритов - трехуровневых однофотонных состояний $|\psi_{m31}\rangle$ и $|\psi_{m32}\rangle$. Как уже отмечалось, комплексные амплитуды вероятностей векторов $|\psi_{m31}\rangle$ и $|\psi_{m32}\rangle$ определяют вероятности срабатывания детекторов приемных оптических модулей ПрОМ-1,2, а также состояние когерентности кубитов, прошедшим по траекториям L_1 и L_2 оптических трактов обоих интерферометров ИМЦ-А,Б.

Контроль когерентности состояний $|\psi_{m31}\rangle$, $|\psi_{m32}\rangle$ необходим для детектирования возможных подмен кубита $|\psi_{m2}\rangle$ простым одноуровневым состоянием $|\psi_0\rangle$. Такая подмена неизбежно приведет к разрушению кубита, а значит и к потере когерентности между $|\psi_{m31}\rangle$ и $|\psi_{m32}\rangle$. Попытки АЕ клонирования целых кубитов из $\mathbf{m}_A$, как было показано, детектируются на логическом уровне протокола.

Для упрощения процедуры контроля, балансировки интерферометров, а также совмещения интерференционного максимума с одним из фотоприемников ПрОМ, в ИМЦ-Б предлагается ввести фазовращающий вентиль, контролирующим фазовый сдвиг ϕ кубитов на траекториях L_1 и L_2. В качестве такого вентиля можно использовать дополнительное ОВ, проложенное вместе с первым волокном по квантовому каналу и соединяющее вторые плечи ИМЦ-А,Б (см. рис. 4.2). Такой прием вдвое увеличивает битрейт $\mathbf{k}_{АБ}$ системы [111].

4.3 Выводы по четвертой главе

Предложен проект системы КРК для протокола BB84 и оптоволоконного квантового канала связи на основе использования временного кодирования двух- и трехуровневых однофотонных квантовых состояний. Рассмотрены логический и физический уровни, показана защищенность протокола как от попыток замены кубитов Евой, так и от просто копирования и передачи полученных состояний.

Особенностью протокола КРК является обязательное включение в обмен сторонами А и Б неконфиденциальной информацией о состояниях с несовпавшими базисами по скоростному классическому каналу, усиливающего его защищенность.

Подмена кубита $|\psi_{m2}\rangle$ в квантовом канале неизбежно приведет к изменению статистического распределения одиночных фотонов по тактовому интервалу. В случае такой подмены $|\psi_{m2}\rangle$ регистрации фотонов возможны в (m-1)-м, m-м, (m+1)-м, (m+2)-м и (m+3)-м тайм-слотах с относительными вероятностями ~ 0.083, 0.25, 0.33, 0.25 и 0.083 соответственно. Контроль указанной статистики позволяет дополнительно усилить защищенность системы.

Вместе с тем, полученные нами результаты представляют решение лишь части задач весьма сложной проблемы. В дальнейшем необходимы решения задач по исследованию границ защищенности данной системы в реальных условиях – помех, диссипации энергии кубитов, возможностей применения квантового помехоустойчивого кодирования и др.

ЗАКЛЮЧЕНИЕ

В ходе диссертационного исследования систем квантового распределения ключа с временным кодированием получены следующие результаты:

1. Модель оценки помехоустойчивости ПрОМ, с использованием работающего в линейном режиме ЛФД, и скорости генерации ключа системы КРК с возможностью варьирования порога срабатывания решающего устройства, позволяющая устанавливать необходимый уровень ложных символов P_f. Показана возможность реализации ПрОМ системы КРК на основе ЛФД Hamamatsu S8664-05K со средней битовой скоростью 10,2 Кб при P_f=7%.

2. Схема контроллера на основе формирователя импульсов напряжения с разрядной линией для ЛФД, работающего в гейгеровском режиме Laser Components G-SPAD SAP500-Series, обеспечивающего длительность импульса на выходе формирователя ~1 нс. Разработан высоковольтный импульсный источник питания по схеме повышающего преобразователя для ЛФД Hamamatsu S8664-05K с выходным напряжением до 500 В и пульсациями не более 18 мВ.

3. Матричный метод описания трансформации квантовых состояний одиночных фотонов в последовательность time-bin кубитов в системе из двух разбалансированных ИМЦ с возможностью ее обобщения на произвольное количество интерферометров. Рассмотрены варианты систем двух разбалансированных ИМЦ, соединенных как одним, так и двумя квантовыми каналами. Показано, что по сравнению с системами КРК с фазовым кодированием второй вариант приготовления и детектирования time-bin кубитов позволяет увеличить системный битрейт в два раза.

4. Симуляционная модель системы КРК с временным кодированием, работающая по протоколу M04. Проведены исследования работы системы с учетом внутренних шумов приемника. Предложены модели подсистем интерферометрического и статистического контроля, приведены результаты симуляций их работы.

5. Метод временного кодирования в системе КРК, работающий по протоколу BB84. Показана возможность детектирования присутствия в системе нелегитимного пользователя за счет контроля статистики срабатывания ПрОМ-1, ПрОМ-2, а также за счет динамического распределения регистрируемых tb-кубитов по тайм-слотам в пределах тактового интервала. Предложено использование данных о состояниях кубитов, не прошедших протокольную процедуру согласования базисов, для усиления защищенности системы.

СПИСОК ЛИТЕРАТУРЫ

1. Дирак П. Принципы квантовой механики. – М.: Наука, Гл. ред. физ.-мат. лит., 1979. – 480 с.
2. Кулик С.Д., Берков А.В., Яковлев В.П. Введение в теорию квантовых вычислений (методы квантовой механики в кибернетике): учебное пособие. Т. 2. М.: МИФИ, 2008. – 532 с.
3. Тахтаджян Л.А. Квантовая механика для математиков. М.-Ижевск: НИЦ "Регулярная и хаотическая динамика", Ижевский институт компьютерных исследований, 2011. — 496 с.
4. McMahon D. Quantum Mechanics Demystified. Mc Graw Hill (USA), 2006. URL: https://kordas.web.cern.ch/kordas/Teaching/FYE40/Material/Quantum_Mechanics_Demystified.pdf (дата обращения: 15.12.2015)
5. Морен К., Методы гильбертова пространства. — М.: Мир, 1965. — 570 с.
6. Холево А.С. Введение в квантовую теорию информации. URL: http://www.rqc.ru/pdf/Holevo3.pdf (дата обращения: 15.12.2015)
7. Килин С.Я., Хорошко Д.Б., Низовцев А.П. Квантовая криптография: идеи и практика. Минск: Белорусская наука, 2008. – 392 с.
8. Shumacher B. Quantum coding // Phys. Rev. A. — 1995. — Vol. 51. — P. 2738.
9. Бауместер Д., Экерт А., Цайлингер А. Физика Квантовой Информации. Пер. с англ. М.: Постмаркет, 2002. – 376 с.
10. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Пер. с англ. М.: Мир, 2006. – 824 с.
11. Белоусов Ю. М. Курс квантовой механики. Нерелятивистская теория. — М.: МФТИ, 2006. — 408 с.
12. Давыдов А. С. Квантовая механика. — М.: Наука, 1973. — 704 с.
13. Имре Ш., Балаж Ф. Квантовые вычисления и связь. Инженерный подход. Пер. с англ. М.: Физматлит, 2008. – 320 с.
14. Емельянов В.И., Владимирова Ю.В. Квантовая физика: биты и кубиты: учеб. пособие. М.: Физический факультет МГУ, 2012. – 176 с.

15. Румянцев К.Е., Голубчиков Д.М. Квантовая связь и криптография: Учебное пособие. Таганрог: ТТИ ЮФУ, 2009. – 122 с.
16. R.P. Feynman The Feynman Lectures on Physics, volume 3, 1965. URL: http://www.feynmanlectures.caltech.edu/III_toc.html (дата обращения: 15.12.2015)
17. Friedman J.R., Patel V., Chen W., Tolpygo S.K., Lurkens J.E. Quantum superposition of distinct macroscopic states. URL: http://www.nature.com/nature/journal/v406/n6791/pdf/406043a0.pdf (дата обращения: 15.12.2015)
18. Mandel L., Wolf E. Optical Coherence and Quantum Optics. Cambridge University Press. 1995. ISBN 0-521-41711-2.
19. Скалли М.О., Зубайри М.С. Квантовая оптика: Пер. с англ. / Под ред. В.В. Самарцева. – М.: ФИЗМАТЛИТ, 2003. – 512 с.
20. Тарасов Л.В. Введение в квантовую оптику. Изд. 2-е. – М.: Изд. ЛКИ, 2008. – 304 с.
21. Wootters W.K., Zurek W.H. A single quantum cannot be cloned // Nature. – 1982. – N. 299. – P. 802-803.
22. Dieks D. Communication by EPR devices. URL: http://dspace.library.uu.nl/handle/1874/16932 (дата обращения 15.12.2015).
23. Иванов М. Г. Как понимать квантовую механику. — М.–Ижевск: НИЦ «Регулярная и хаотическая динамика», 2012. — 516 с.
24. Лоудон Р. Квантовая теория света. - М.: Мир, 1976. - 488 с.
25. Гринштейн Дж., Зайонц А. Квантовый вызов. - М.: Интеллект. 2008 г. – 400 с.
26. Ulf L. Measuring the quantum state of light / Cambridge University Press. - 2005. – 208p.
27. Прескилл Дж. Квантовая информация и квантовые вычисления. Т. 1. М. – Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2008. – 464 с.

28. Прескилл Дж. Квантовая информация и квантовые вычисления. Т. 2. М. – Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2011. – 312 с.
29. Сивухин Д.В. Общий курс физики. Оптика. URL: https://mipt.ru/dasr/upload/89a/f_3kf3p7-arphh81ii9w.pdf (дата обращения: 15.12.2015)
30. Sharma K. K. Optics: principles and applications. — Academic Press, 2006. — 638 p.
31. Marcikic I. и другие. Femtosecond Time-bin entangled qubits for quantum communication. URL: http://arxiv.org/pdf/quant-ph/0205144v2.pdf (дата обращения: 06.12.2015).
32. Bennett C. H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers and Systems and Signal Processing (Bangalore, India). — 1984. — P. 175–179.
33. Bennett C.H. Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. —1992. —Vol. 68. — P. 3121.
34. Huttner B., Imoto N. Gisin N., Mot T. Quantum cryptography with coherent states // Phys. Rev. A. — 1995. — Vol. 51. — P. 1863.
35. Bruss D. Optimal Eavesdropping in Quantum cryptography with Six States // Phys. Rev. Lett. — 1998. — Vol. 81. — P. 3018.
36. Goldenberg L., Vaidman L. Quantum cryptography based on orthogonal states // Phys. Rev. Lett. — 1995. — Vol. 75. — P. 1239
37. Koashi M., Imoto N. Quantum cryptography based on split transmission of one-bit information in two steps // Phys. Rev. Lett. — 1997. — Vol. 79. — P. 2383
38. Ekert A. Quantum cryptography based on Bells theorem // Phys. Rev. Let. — 1991. — Vol. 67, № 6. — P. 661-663.
39. Bennett C., Bessette F., Brassard G., Salvail L. and Smolin J. Experimental quantum cryptography // J. Cryptology. — 1992. — Vol. 5. — P. 3-28

40. Muller. A., Breguet J. And Gisin N. Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km // Europhysics Lett. — 1993. — Vol. 23. — P. 383-388.
41. Breguet J., Muller A., Gisin N. Quantum cryptography with polarized photons in optical fibers: experimental and practical limits // J. Mod. Opt. — 1994. — Vol. 41. — P. 2405-2412.
42. Muller A., Zbinden H. and Gisin N. Underwater quantum coding // Nature. — 1995. — Vol. 378. — P. 449
43. Muller A., Zbinden H. and Gisin N. Quantum cryptography over 23 km in installed under-lake telecom fiber // Europhysics Lett. — 1996. — Vol. 33. — P. 335-339.
44. Marand C. and Townsend P. Quantum key distribution over distances as long as 30 km // Opt. Lett. — 1995. — Vol. 20. — P. 1695-1697.
45. Townsend P. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fiber using wavelength-division multiplexing // Electronics Lett. — 1997. — Vol. 33. — P. 188-190.
46. Townsend P. Quantum cryptography on multiuser optical fibre networks // Nature. — 1997. — Vol. 385. — P. 47-49.
47. Townsend P. Quantum cryptography on optical fiber networks // Opt. Fiber. Tech. —1998. — Vol. 4. — P. 345-370.
48. Hughes R., Morgan G. and Peterson C. Practical quantum key distribution over a 48 km optical fiber network // J. Mod. Opt. — 2000. — Vol. 47. — P. 533-547.
49. Hiskett P., Bonfrate G., Buller G. and Townsend P. Eighty kilometer transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55nm // J. Mod. Opt. — 2001. — Vol. 48. — P. 1957-1966.
50. Kimura T., Nambu Y., Hatanaka T., Tomita A., Kosaka H. and Nakamura K. Single-photon interference over 150km transmission using silica-based integrated optic interferometers for quantum cryptography // Jpn. J. Appl. Phys. — 2004. — Vol. 43. — L1217-L1219.

51. Gobby C., Yuan Z. and Shields A. Quantum key distribution over 122km of standard telecom fiber // Appl. Phys. Lett. — 2004. — Vol. 84. — P. 3762-3764.
52. Takesue H., Diamanti E., Honjo T., Langrock C., Fejer M. Inoue K. and Yamamoto Y. Differential phase shift quantum key distribution experiment over 105km fiber // New J. Phys. — 2005. — Vol. 7. — P. 232.
53. Hiskett P., Rosenberg D., Peterson C., Hughes R., Nam S., Lita A., Miller A. and Nordholt J. Long-distance quantum key distribution in optical fiber // New J. Phys. — 2006. — Vol. 8. — P. 193.
54. Голубчиков Д., Румянцев К. Квантовая криптография: принципы, протоколы, системы. URL: http://www.ict.edu.ru/ft/005712/68358e2-st14.pdf (дата обращения 17.12.2015)
55. Ursin R., Tiefenbacher F., Schmitt-Manderbach T. and other Free-space distribution of entanglement and single photons over 144 km, 2006. URL: http://lanl.arxiv.org/ftp/quant-ph/papers/0607/0607182.pdf (дата обращения 17.12. 2015)
56. Schmitt-Manderbach T. and other Experimental demonstration of free-space decoy-state quantum key distribution over 144 km // Phys. Rev. Lett. — 2007. — Vol. 98. — P. 1010504.
57. Dixon A., Yuan Z., Dynes J. Sharpe A. and Shields A. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate // Optics Express. — 2008. — Vol. 16, Issue 23. — P. 18790-18979.
58. Lucamarini M., Patel K. and other Efficient decoy-state quantum key distribution with quantified security. URL: https://www.osapublishing.org/view_article.cfm?gotourl=https%3A%2F%2Fwww%2Eosapublishing%2Eorg%2FDirectPDFAccess%2FD97DD14E-A11D-9FFE-A76760630BBE764C_268752%2Foe-21-21-24550%2Epdf%3Fda%3D1%26id%3D268752%26seq%3D0%26mobile%3Dno&org= (дата обращения 17.12.2015)

59. Toshiba QKD system. URL: http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution/Toshiba-QKD-system/
60. Korzh B., Ci Wen Lim C. and other Provably secure and practical quantum key distribution over 307 km of optical fibre. URL: http://arxiv.org/pdf/1407.7427v1.pdf (дата обращения 17.12.2015)
61. Quantum key distribution, standarts. URL http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution (дата обращения 18.12.2015)
62. Metrology for Industrial Quantum Commucation. URL: http://projects.npl.co.uk/MIQC/index.html (дата обращения 18.12.2015)
63. Кронберг Д.А. и др. Квантовая криптография. Учебное пособие. URL: http://sqi.cs.msu.su/store/storage/ss8dw5n_quantum_cryptography.pdf (дата обращения 06.12. 2015).
64. Shor P.W. Simple proof of security of the BB84 quantum key distribution protocol / P.W. Shor, J. Preskill // Phys. Rev. Lett. — 2000. — Vol. 85. — P. 441.
65. Прокис Дж. Цифровая связь. Пер. с англ. - М.: Радио и связь, 2000. - 797 с.
66. Brassard G. Limitations on practical quantum cryptography / G. Brassard, N. Lütkenhaus, T. Mor, B.C Sanders // Phys. Rev. Lett. – 2000. – Vol. 85. – P. 1330–1333.
67. Стиб В.-Х., Харди Й. Задачи и их решения в квантовых вычислениях и квантовой теории информации. Москва-Ижевск, «Регулярная и хаотическая динамика», 2007. 296 с.
68. Хелстром К., Квантовая теория проверки гипотез и оценивания, М.: Мир 1978. - 344 с.
69. Ivanovic I. D. How to differentiate between non-orthogonal states // Phys. Lett. A. 123, 257–259 (1987).
70. Clarke R.B.M., Chefles A., Barnett S.M. and Riis E. Experimental demonstration of optimal unambiguous state discrimination // Phys. Rev. 2001. Vol. 63, Iss. 4. 040305.

71. Maslennikov G. Practical realization of quantum cryptography protocol exploiting polarization encoding in qutrits / G. Maslennikov, A. Zhukov, M. Chekhova and S. Kulik // Journal of Optics B. – 2003. – Vol. 5, № 4. – P. 530–534.
72. Молотков С. Н. Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы // Письма в ЖЭТФ. — 2004.— Т. 79.— С. 691–704.
73. Debuisschert T., Boucher W. Time coding protocols for quantum key distribution // Phys. Rev. A. – 2004. – Vol. 70, Iss. 4. – P. 042306.
74. Молотков С.Н. Мультиплексная квантовая криптография с временным кодированием без интерферометров // Письма в ЖЭТФ. – 2004. – Т. 79, вып. 9. – С. 554–559.
75. Lo H.-K., Ma X., Chen K. Decoy state quantum key distribution // Phys. Rev. Let. – 2005. – Vol 94. – P. 230504.
76. Хорошко Д.Б., Пустоход Д.И., Килин С.Я. Квантовое распределение ключа на временных сдвигах с использованием состояний-ловушек // Оптика и спектроскопия. – 2010. – Т. 108, вып. 3. – С. 372–379.
77. Хорошко Д.Б., Пустоход Д.И., Килин С.Я. Квантовое распределение ключа на временных сдвигах: чувствительность к потерям // Оптика и спектроскопия. – 2011. – Т. 111, вып. 5. – С. 719–723.
78. Хорошко Д.Б., Пустоход Д.И., Килин С.Я. Квантовое распределение ключа с кодированием по времени на линейно зависимых состояниях // Оптика и спектроскопия. – 2012. – Т. 112, вып. 3. – С. 373–380.
79. Розеншер Э., Винтер Б. Оптоэлектроника - М.: Техносфера, 2004. - 592 с.
80. Avalanche photodiodes and quenching circuits for single-photon detection / S. Cova, M. Ghioni, A. Lacaita, C. Samori, F. Zappa // Applied Optics. –1996. – Vol. 35, No. 12. – P 1956-1976.
81. Duarte F.J. Laser Pulse Phenomena and Applications. URL: http://www.twirpx.com/file/502972/ (дата обращения 09.12.2012)

82. Fishburn M.W. Fundamental of CMOS single-photon avalanche diodes. – Delft: Delft University of Technology. – 2012. – 165 pp.
83. Keiser G. Optical Fiber Communications – New York : McGraw-Hill Inc., 1991. – 461 p.
84. Задорин А.С., Максимов А.В., Махорин Д.А. и др. Скорость генерации кода в системе квантового распределения ключей // Доклады ТУСУРа. – 2011. – № 2 (24). – С. 139-141
85. Задорин А.С., Максимов А.В., Махорин Д.А. Режимы работы фотоприемного устройства системы квантовой криптографии // Доклады ТУСУРа. – 2012. - № 2 (26). – С. 63-66.
86. Данные о кремниевом лавинном диоде S8664 серии. URL: http://sales.hamamatsu.com/assets/pdf/parts_S/S8664_series.pdf (дата обращения 17.09.2012).
87. Махорин Д.А., Галиев А.Б., Задорин А.С. Возможность реализации линейного режима счета фотонов на лавинном фотодиоде S8664-05K при комнатной температуре // Доклады ТУСУРа. – 2014. - № 1 (31). – С. 65-68.
88. Данные о микросхеме LM5022 фирмы Texas Instrument. URL: http://www.ti.com/lit/ds/symlink/lm5022.pdf (дата обращения 15.05.2013).
89. Браун М. Источники питания. Расчет и конструирование. Перевод с англ. – К.: МК-Пресс, 2007. – 288 с.
90. Конкин Д.А., Максимов А.В., Махорин Д.А. Высоковольтный источник питания лавинного фотодиода, работающего в режиме счета фотонов // Известия высших учебных заведений. Физика. – 2013. – Т. 56, вып. 9-2. – С 34-36.
91. Авдоченко Б.И., Ильюшенко В.Н., Тулеев А.В., Цепелев Г.М. Многофункциональный генератор для пикосекундных время-импульсных радиотехнических систем. Труды IV международной конференции "Актуальные проблемы электронного приборостроения" // Новосибирск. – 1998. – т.10. – с. 99-102. /

92. Введение в Multisim. National Instriments. URL: ftp://ftp.ni.com/pub/branches/russia/software/multisim_gettingstarted.pdf (дата обращения 18.12.2015)
93. Хернитер М. Самоучитель по Electronics Workbench Multisim. М.: Издательство дом ДМК пресс, 2006. – 488с.
94. Данные о кремниевом лавинном диоде, с гейгеровским режимом URL: http://www.lasercomponents.com/de/?embedded=1&file=fileadmin/user_upload/home/Datash eet/l cd/sap-series.pdf&no_cache=1 (дата обращения: 17.09.2012).
95. Махорин Д.А. Особенности гейгеровского режима работы фотоприемного устройства системы КРК // Материалы докладов XVII Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР – 2012», г. Томск, 16-18 мая 2012г.
96. Авдоченко Б.И., Задорин А.С., Максимов А.В., Махорин Д.А. Контроллер лавинного фотодиода системы квантовой криптографии // Материалы докладов VIII Международной научно-практической конференции «Электронные средства и системы управления» Томск. – 2012. – Ч.2. – С. 105-109.
97. Ziemann O., Krauser J., Zamzow P., and Daum W. POF-Handbook: Short Range Optical Transmission Systems, 2nd ed. Berlin, Germany: Springer-Verlag, 2008.
98. Даташит микросхемы контроллера лазерного диода http://www.ti.com/lit/ds/symlink/onet4201ld.pdf
99. Даташит усилительного тракта ПрОМ http://www.avagotech.com/docs/AV02-1502EN
100. Даташит усилителя-ограничителя http://www.ti.com.cn/cn/lit/ds/symlink/onet4201pa.pdf
101. Задорин А.С., Махорин Д.А. Матричное описание трансформации квантовых состояний одиночных фотонов в последовательности разбалансированных интерферометров Маха-Цендера // Доклады ТУСУРа. – 2015. – №3 (37). – С. 145-149.

102. Дьяконов В. П. Simulink 5/6/7. Самоучитель. –М.: ДМК-Пресс, 2008. – 784 с.
103. Черных И.В. Simulink: Инструмент моделирования динамических систем. URL: http://matlab.exponenta.ru/simulink/book1/ (дата обращения 18.12.2015)
104. Задорин А.С., Махорин Д.А. Модель системы квантового распределения ключей по оптическому волокну с временным кодированием // Доклады ТУСУРа. – 2014. – № 3(33). – С. 85-89.
105. Свид. о государственной регистрации программы для ЭВМ №2015617171. Махорин Д.А., Задорин А.С. Quantum key distribution system. Зарег. в Реестре программ для ЭВМ 2 июля 2015 г.
106. Задорин А.С., Махорин Д.А. Статистическая обработка сигналов в системах квантового распределения ключа // Доклады ТУСУРа. – 2014. – №3 (33). – С. 90–93.
107. Махорин Д.А., Задорин А.С., Решетников С.Ю. Статистический контроль распределения числа фотонов в информационных сообщениях в системе квантового распределения ключа с временным кодированием // Материалы докладов XI Международной научно-практической конференции «Электронные средства и системы управления - 2014» – Томск, 25-27 ноября 2015г. Часть. 1. – С. 270-273.
108. Задорин А.С., Махорин Д.А. Интерферометрический контроль целостности данных в системе квантового распределения ключей с временным кодированием // Доклады ТУСУРа. – 2014. – № 4 (34). – С. 85–88.
109. Махорин Д. А., Задорин А. С., Альбрехт Р. С., Исатаев А. Н. Усиление защищенности системы квантового распределения ключа с временным кодированием по оптическому волокну // Международная конференция «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2015), материалы 25-й международ. конф. – Севастополь, 2015. том 1 – С. 1019-1021.
110. Зайдель А.Н. Ошибки измерений физических величин: Учебное пособие. СПб.: Издательство «Лань», 2009, - 112 с.

111. Задорин А.С., Махорин Д.А. Временное кодирование состояний фотонов в системе квантового распределения ключей с временным кодированием tb-кубитов // Материалы докладов XI Международной научно-практической конференции «Электронные средства и системы управления - 2014», г. Томск, 25-27 ноября 2015г. Часть. 1. С. 265-269.

ПРИЛОЖЕНИЯ А

УТВЕРЖДАЮ
Проректор по учебной работе ТУСУР,
д.т.н., профессор
_____ Троян П.Е.
«__» 03 _____ 2016г.

АКТ

внедрения в учебный процесс результатов диссертационной работы

Махорина Дмитрия Алексеевича

Настоящий акт подтверждает факт внедрения результатов диссертационной работы Махорина Дмитрия Алексеевича «Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи» в учебный процесс кафедры «Радиоэлектроники и защиты информации (РЗИ)» радиотехнического факультета (РТФ) ТУСУРа (г. Томск).

В диссертационной работе Махориным Д.А. разработана программная модель системы квантового распределения ключа с временным кодированием по протоколу M04, а также подсистемы интерферометрического и статистического контроля целостности передаваемых данных для указанной модели.

Указанные результаты использованы в учебном процессе каф. РЗИ в течение зимних и весенних семестров 2014-2016 гг. при подготовке студентов в рамках основных образовательных программ кафедры: бакалаврские программы 10.03.01 «Информационная безопасность» и 10.03.02 «Инфокоммуникационные технологии и системы связи», профиль «Защищенные системы и сети связи», а также в магистерской программе "Системы и устройства передачи, приема и обработки сигналов" направления 11.04.01 «Радиотехника», по дисциплинам:

- Научно-исследовательская работа;
- Государственная итоговая аттестация;
- Защита информационных процессов в системах связи;
- Групповое проектное обучение в рамках проекта РЗИ-1401 «Квантовая криптография»

Заведующий каф. РЗИ _____ Задорин А.С

Декан РТФ _____ Попова К.Ю.

Ростелеком

Публичное акционерное общество междугородной и международной электрической связи «Ростелеком»

МАКРОРЕГИОНАЛЬНЫЙ ФИЛИАЛ «СИБИРЬ»

ТОМСКИЙ ФИЛИАЛ

пр. Фрунзе, д. 83а
г.Томск, Россия, 634061
Тел.: 8 (3822) 52-38-63, Факс: 8 (3822) 25-91-04
e-mail: info@sibir.rt.ru, web: www.rt.ru

УТВЕРЖДАЮ
Заместитель директора филиала-
Технический директор

_____ Л.Ю. Шурыгин

«11» 03 2016г.

Акт внедрения (использования) результатов
диссертационной работы Махорина Дмитрия Алексеевича

Настоящий акт подтверждает использование результатов кандидатской диссертационной работы Махорина Дмитрия Алексеевича на тему «Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи» в Томском филиале ПАО «Ростелеком» в части:

1) Обзор актуальных разработок в области квантового распределения ключа;

2) Модель системы квантового распределения ключей с временным кодированием по протоколу M04 с подсистемами интерферометрического и статистического контроля целостности передаваемых данных.

Данные результаты представляют практический интерес ПАО «Ростелеком» в связи с развитием корпоративной политики по внедрению перспективных систем защищенной связи.

Заместитель технического
директора по эксплуатации С.В. Ховрин

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2015617171

«Quantum key distribution system»

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Томский государственный университет систем управления и радиоэлектроники» (RU)***

Авторы: ***Махорин Дмитрий Алексеевич (RU),***
Задорин Анатолий Семенович (RU)

Заявка № **2015612779**
Дата поступления **09 апреля 2015 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***02 июля 2015 г.***

Врио руководителя Федеральной службы по интеллектуальной собственности

Л.Л. Кирий

ПРИЛОЖЕНИЕ Б

Модель для оценки помехоустойчивости

$h := 6.62 \cdot 10^{-34}$ $k := 1.38 \cdot 10^{-23}$ постоянные Планка и Больцмана

$q := 1.6 \cdot 10^{-19}$ заряд электрона

$t := 293$ абсолютная температура (К)

$\lambda := 0.55 \cdot 10^{-6}$ длина световой волны (мкм)

$\nu := 3 \cdot \frac{10^8}{\lambda}$ частота световой волны (мкм)

$\nu = 5.455 \times 10^{14}$

Расчет средней мощности сигнала Pc

$\tau 0 := 2 \cdot 10^{-9}$ длительность сигнального импульса (с)

$\tau 0 = 2 \times 10^{-9}$

$Po := h \cdot \frac{\nu}{\tau 0}$ мощность сигнального импуль $Po = 1.805 \times 10^{-10}$

$B0 := 1 \cdot 10^6$ битовая скорость СП (бит/с)

$T0 := \frac{1}{B0} = 1 \times 10^{-6}$ длительность тактового интервала (с)

$\xi 1 := \frac{\tau 0}{T0} = 2 \times 10^{-3}$ ξ1 -длительность сигнального импульса,отно сительно T0

$\zeta := 15$ ζ-заданный допуск на уширение сигнального импул са в тракте ФПУ,вследствие ограничения полосы час тот

$T := \zeta \cdot \tau 0 = 3 \times 10^{-8}$ длительность уширенного сигнала на входе ПУ (с)

$\xi := \frac{T}{T0} = 0.03$ ξ-длительность импульса T на выходе ФПУ ,относительно T0

$B := \frac{1}{T} = 3.333 \times 10^7$ оценка для полосы частот тракта ФПУ (Гц.)

Распределение Гаусса $Pg(u, uo, \sigma) := \frac{1}{\sigma \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left[-\frac{(u - uo)^2}{2 \cdot \sigma^2} \right]$

$nc := 0.1$ среднее число фооэлектронов

$Pc := nc \cdot Po$ средняя мощность сигнала $Pc = 1.805 \times 10^{-11}$

$Ls := 1$ длина линии передачи (км)

$\alpha := 9$ коэффициент затухания сигнала в тракте СП (дБ /км)

$Pc := Pc \cdot 10^{\frac{-(\alpha \cdot Ls)}{10}}$ средний уровень сигнала на входе премника системы КРК $Pc = 1.795 \times 10^{-11}$

Расчет помехоустойчивости системы КРК

$\chi := 500$ — χ - предискажения сигнального импулса в тракте ФПУ за счет противошумовой корреции ФПУ

$C := 1.5 \cdot 10^{-12}$ — C - емкость фотодиода

$R := \frac{\chi}{2 \cdot C \cdot B} = 5 \times 10^{6}$ — R - сопротивление нагрузки ЛФД

$R := 5 \cdot 10^{6}$

$itt := 0.15 \cdot 10^{-9}$ $\eta := 0.78$ — темновой ток (А), квантовая эффективность ЛФД

$M := 100$ — коэффициент лавинного размножения ЛФД

$ntt := \left(itt \cdot \frac{T}{q} \right) = 28.125$ — число шумовых фотоэектронов темнового тока на измерительном интервале T

Параметры предварительного усилителя ФПУ

$qm := 40 \times 10^{-3}$ $Iin := 1 \times 10^{-12}$ $\Gamma d := 3$

qm, Г - крутизна (Сим), ток утечки затвора (А) и коэффициент шума (дБ) полевого танзистора

$\Gamma := e^{\frac{\log(\Gamma d)}{10}}$ $\Gamma = 1.049$ — Г, - коэффициент шума полевого транзистора в первом каскаде ОУ

$Sai := 2 \cdot q \cdot Iin$ $Sae := \frac{4 \cdot k \cdot t \cdot \Gamma}{qm}$ Sai, Sae - эквивалентные шумовые источники

$I2(\theta) := \frac{2}{\pi} \cdot \int_0^{\frac{\pi}{2}} e^{16 \cdot \theta^2 x^2} \cdot (\cos(x))^4 \, dx$ — Второй интеграл Персоника

$I2(\xi) = 0.376$

$I3(\theta) := \left(\frac{2}{\pi} \right)^3 \cdot \int_0^{\frac{\pi}{2}} e^{16 \cdot \theta^2 x^2} \cdot x^2 \cdot (\cos(x))^4 \, dx$ — Третий интеграл Персоника

$I3(\xi) = 0.03$

$W := \frac{I2(\xi)}{\left(q^2 \cdot B\right)} \cdot \left(Sai + \frac{4 \cdot k \cdot t}{R} + \frac{Sae}{R^2} \right) + Sae \cdot \frac{4 \cdot \pi^2 \cdot C^2 \cdot B \cdot I3(\xi)}{q^2} = 2.909 \times 10^{3}$

W-безразмерный температурный шумовой параметр усилителя ФПУ

Dr-безразмерный параметр,характеризующий дробовые шумы ЛФД

$Dr := I2(\xi)\cdot ntt = 10.577$

Проверка

$\frac{I2(\xi)}{\left(q^2\cdot B\right)}\cdot\left(\frac{4\cdot k\cdot t}{R}\right) = 1.426\times 10^{3}$ $\qquad$ $\frac{I2(\xi)}{\left(q^2\cdot B\right)}\cdot\left(\frac{Sae}{R^2}\right) = 7.476\times 10^{-3}$

$\frac{I2(\xi)}{\left(q^2\cdot B\right)}\cdot(Sai) = 0.141$ $\qquad$ $Sae\cdot\frac{4\cdot\pi^2\cdot C^2\cdot B\cdot I3(\xi)}{q^2} = 1.483\times 10^{3}$

$N := \sqrt{(Dr + W)} = 54.032$ $\qquad$ $\sqrt{(W)} = 53.934$

$Pn(n) := Pg(n, 0, N)$ **Суммарное распределение шумов** P(n)

$Pc(n) := Pn(n - M)$ **Распределение смеси сигнала и шума** Pc(n)

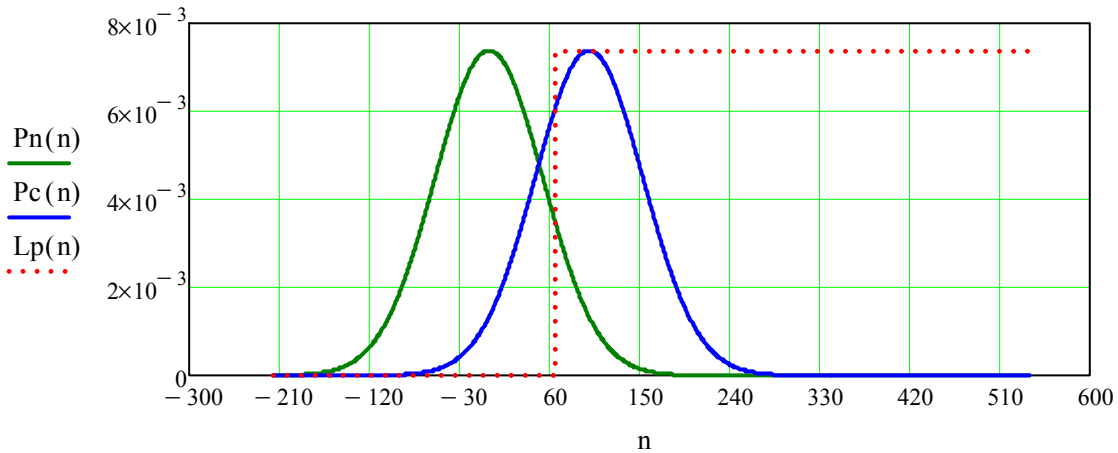
$L := 66.5$ **Пороговый уровень сигнала** L

$n := -4(N) .. 10N$ $\qquad$ $\int_{-5N}^{5N} Pn(n)\,dn = 1$ $\qquad$ $\int_{-5N}^{5N} Pc(n)\,dn = 0.999$

$Pf := \int_{L}^{5N} Pn(n)\,dn = 0.109$ **Вероятность ложного сигнала** Pf(n)

$Pl := \int_{-5N}^{L} Pc(n)\,dn = 0.268$ **Вероятность пропуска сигнала** Pl(n)

$(\Lambda(n) := if(n \geq 0, 1, 0))$ $\qquad$ $(Lp(n) := \Lambda(n - L)\cdot Pn(0))$



Расчет битовой скорости формирования КРК, бит/с. Bp

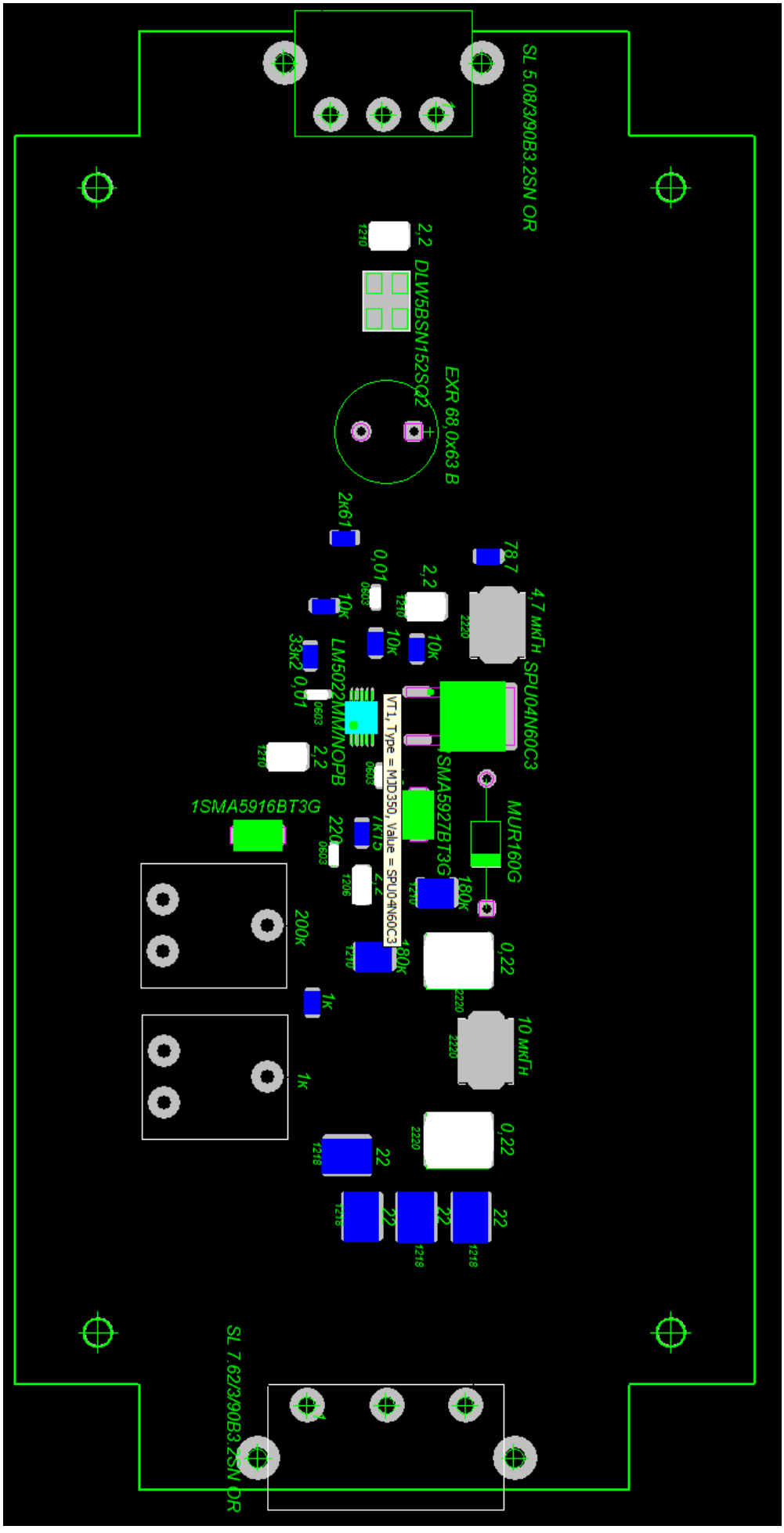
Kpr := 0.25 протокольный коэффициент снижения скорости Kpr,

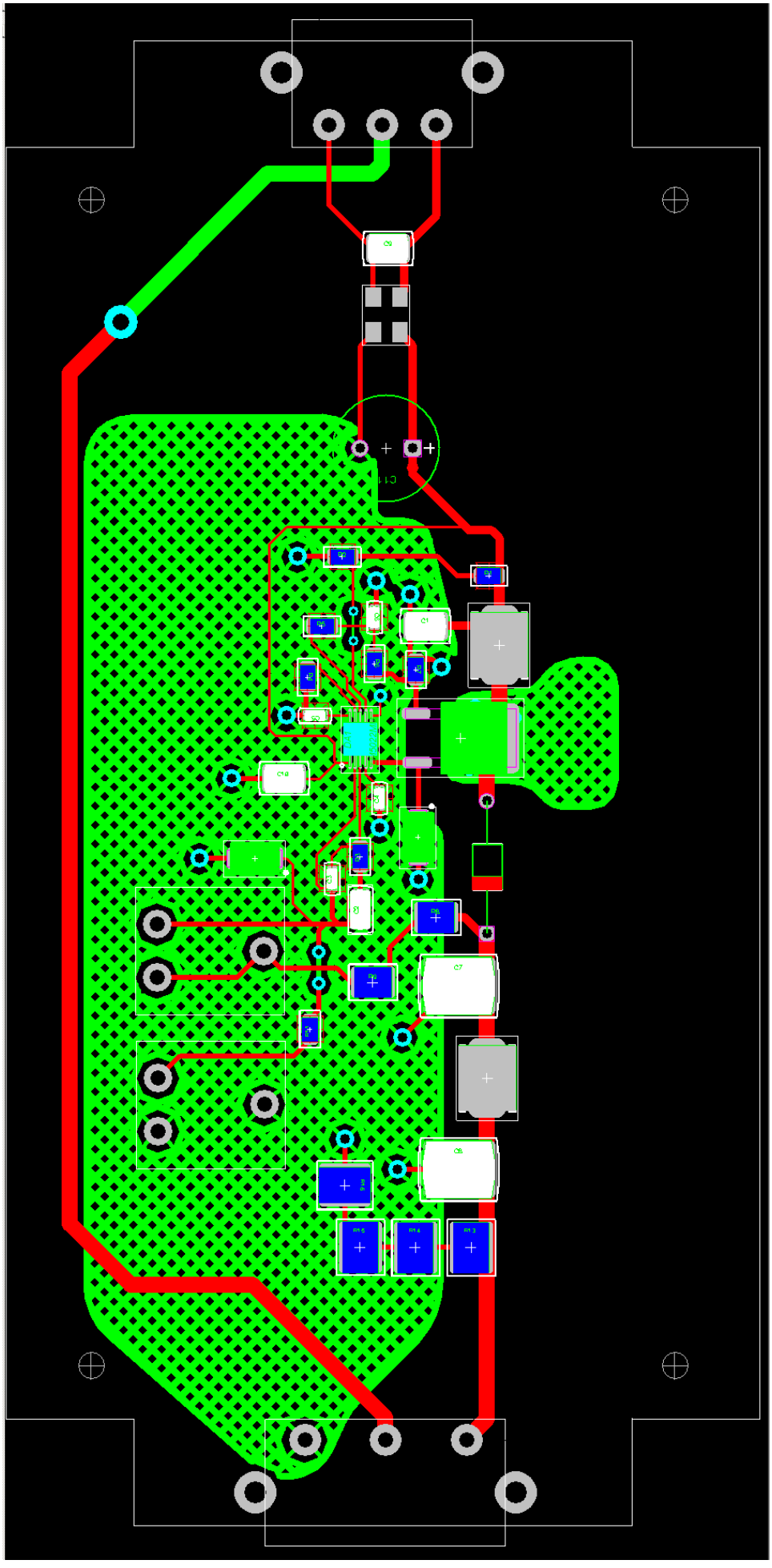
$$Bp := B0 \cdot (1 - Pl) \cdot nc \cdot Kpr \cdot 10^{\frac{-(\alpha \cdot Ls)}{10}} = 2.315 \times 10^{3}$$

ПРИЛОЖЕНИЕ В

	Конденсаторы (MURATA) GRM		
C1	*2,2 мкф+/- 10% (GRM32ER72A225KA35)*	*1*	
C2	*2,2 мкф+/- 10% (GRM31CR71H225KA88)*	*1*	
C3	*220 пф+/- 5% (GRM1882C2A221KA01)*	*1*	
C4	*1 мкф+/- 10% (GRM188R71E105KA12)*	*1*	
C5, C6	*10000 пф+/- 10% (GRM188R71H103KA01)*	*2*	
C7, C8	*0,22 мкф +/- 10% (GRM55DR72J224KW01)*	*2*	
C9, C10	*2,2 мкф +/- 10% (GRM32ER72A225KA35)*	*2*	
C11	*Электролит EXR 68 мкф 63 в (HITANO)*	*1*	
	Микросхемы		
DA1	*LM5022MM (National Semiconductor)*	*1*	
	Индуктивности (MURATA)		
L1	*4700 мкГ+/-20% (LQH55DN472M03)*	*1*	
L2	*10 мкГ+/-20% (LQH55DN100M03)*	*1*	
L3	*DLW5BSN152SQ2*	*1*	
	-		
	Резисторы VISHAY CRCW		
R1	*78,7 ком+/-1% 0805 78K7FK*	*1*	
R2	*2,61 ком+/-1% 0805 2K61FK*	*1*	
R3	*7,15 ком+/-1% 0805 7K15FK*	*1*	
R4	*33,2 ком+/-1% 0805 33K2FK*	*1*	
R5…R7	*10 ком+/-1% 0805 10K0FK*	*3*	

R8, R9	*180 ком+/-5% 1210 180KJN*	*2*	
R11	*1 ком+/-1% 0805 1K00FK*	*1*	
R13...R16	*22 ком+/-5% 1218 22K0JN*	*4*	
	-		
	Резисторы переменные (АСР)		
R10	*200 ком+/-20% MCA9V10*	*1*	
R12	*1 ком+/-20% MCA9V10*	*1*	
	-		
	Диоды		
VD1	*Диод защитный 1SMA5927BT3G (ONS)*	*1*	
VD2	*MUR160G (ONS)*	*1*	
VD3	*1SMA5916BT3G (ONS)*	*1*	
	-		
	Транзисторы		
VT1	*SPU04N60C3 (INFINEON)*	*1*	
	-		
	Разъемы		
XP1	*Weidmuller SL 5,08/3/90B3.2 SNOR*	*1*	
XP2	*Weidmuller SL 7,62/3/90B3.2 SNOR*	*1*	


SL 5.08/3/90B3.2SN OR
2,2
1210
DLW5BSN152SQ2
EXR 68,0x63 B
2к61
0,01
0603
78,7
2,2
1210
2220
4,7 мкГн
SPU04N60C3
10к
10к
10к
33к2
0,01
0603
LM5022MM/NOPB
2,2
1210
0603
VT1, Type = MJD350, Value = SPU04N60C3
SMA5927BT3G
MUR160G
1SMA5916BT3G
220
0603
7к15
2,2
1206
180к
1210
180к
1210
0,22
2220
200к
1к
10 мкГн
2220
1к
22
1218
0,22
2220
22
1210
22
1218
22
1218
SL 7.62/3/90B3.2SN OR



ПРИЛОЖЕНИЕ Г

1.1 Интерферометр ПА

```
function [z,x,c]=fcn(b,a) % Функции путей фотона
z=0;
x=0;
c=0;
if b==0                   % Прохождение фотона по короткому пути
z=a;
end
if b==1                   % Прохождение фотона по длинному пути
c=a;
end
if b==2                   % Прохождение фотона по обоим путям одновременно
x=a;
c=a;
end
end
```

1.2 Интерферометр ПБ

```
function [z,x,c]=fcn(b,a) % Функция путей фотона
z=0;
x=0;
c=0;
p=a;
if b==0 & p<1.2           % Прохождение фотона по короткому пути
z=p;
end
if b==1 & p<1.2           % Прохождение фотона по длинному пути
c=p;
end
if b==2 & p<1.2           % Прохождение фотона по обоим путям одновременно,
x=p;
c=p;
end
if p==1.2 & b==0          % Прохождение фотона по короткому пути после перехвата
z=p;
end
if p==1.2 & b==1          % Прохождение фотона по короткому пути после перехвата
z=p;
end
if p==1.2 & b==2          % Прохождение фотона по длинному после перехвата
c=p;
end
end
```

1.3 Имитация устройства распределения

```
function [y,x] = fcn(u1,u2,u3) % Функция устройства распределения
l=u1;                          % Объявление переменной градуса ФИ
k=u2;                          % Объявление переменной
                               % процента попадания на ПрОМ 1 и 2
m=u3;                          % Объявление переменной потока фотонов
y=0;                           % Объявление переменной выхода на ПрОМ 1
x=0;                         % Объявление переменной выхода на ПрОМ 2
r=(l*3.14)/180;              % Функция перевода из градусов в радианы
c=(cos(r)^2)*100;            % Функция cos^2(x)
```

```
s=(sin(r)^2)*100;           % Функция sin^2(x)

if k<c & m<1.2              % Условие прохождение фотона на ПрОМ 1
        y=m;
        x=0;
end
    if k>c & m<1.2          % Условие прохождение фотона на ПрОМ 2
        y=0;
        x=m;
    end

    if m==1.2 & k>49        % Условие прохождение фотона на ПрОМ 1 при перехвате
        y=m;
        x=0;
    end
    if m==1.2 & k<49        % Условие прохождение фотона на ПрОМ 2 при перехвате
        y=0;
        x=m;
    end
end
```

1.4 Интерферометрический контроль

```
function [y,x] = fcn(FD_1,FD_2,grad) % Функция подсчета количества срабатываний
ПрОМ 1 и ПрОМ 2
A=FD_1;                             % Объявление переменной входа ПрОМ 1
B=FD_2;                             % Объявление переменной входа ПрОМ 2
k=grad;                             % Объявление переменной входа градуса ФИ
m=0;
o=0;
u=0;
C=A+B;
AA=(A*100)/C;                       % Функция подсчета процента попадания фотонов
на ПрОМ 1
BB=(B*100)/C;                       % Функция подсчета процента попадания фотонов
на ПрОМ 2
x=AA                                % Вывод результата на вход 1
y=BB                                % Вывод результата на вход 2
n=o
t=u
```

1.5 Блок АЕ

```
function x = fcn(A,B)           % Функция имитиции перехвата Евы
n=length(A);                    % Общее количество фотонов
i=1:n;
coder.extrinsic('disp')
disp(' i A(i)')
k=0;
x=0;
for i=1:1:n                     % Цикл проверки условий на случайный коллапс
фотона в одно из состояний
if B==0                         % Условие при
if A(i)< 1.2 & A(i)> 1.07       % Условие коллапса для короткого пути
A(i)=1.2;
x=A(i);
end
if A(i)< 1.07 & A(i)> 1.02      % Условие запрета прохождения фотона по длинному
пути
```

```
A(i)=0;
x=A(i);
end
end
if B==1                          % Условие коллапса для длинного пути
if A(i)< 1.2 & A(i)> 1.07        % Условие запрета прохождения фотона по короткому
пути
A(i)=0;
x=A(i);
end
if A(i)< 1.07 & A(i)> 1.02       % Условие разрешения прохождения фотона по длинному
пути
A(i)=1.2;
x=A(i);
end
end
if A(i)==1
A(i)=1.2;
x=A(i);
end
end
```

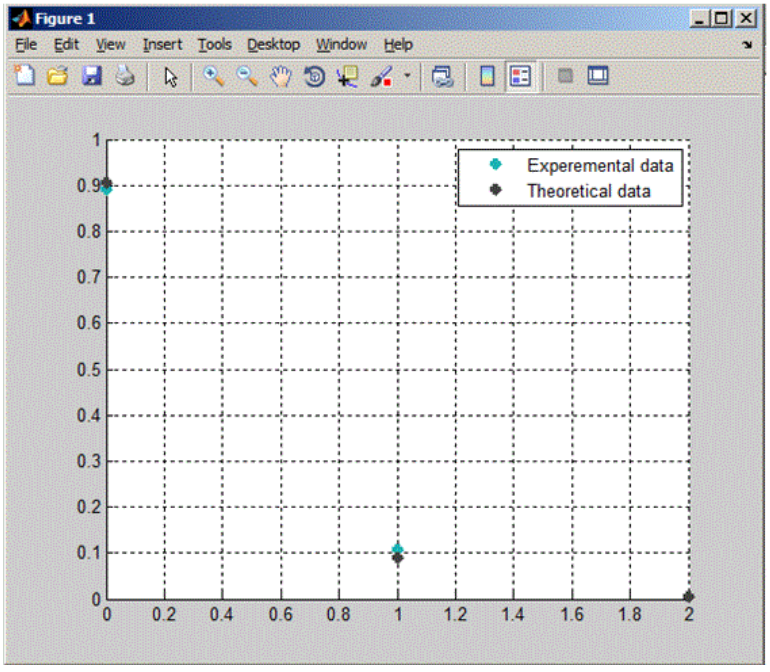
2.1 Статистический контроль

```
count=0;
count1=0;
size=10000;
size_window=10; %Размерность окна
iter_0=1;
iter_1=1; %Переменная для подсчета однофотонных посылок
iter_2=1; %Переменная для подсчета двухфотонных посылок
iter_3=1; %Переменная для подсчета трехфотонных посылок
b=size/size_window; % Количество окон
for i=1:1:10000  % Цикл проверки всего массива
    count=count+1;
    if simout(i)==1  % Подсчет фотонов
        count1=1+count1;
    end;
    if count ==10 % Когда окно закончилось, происходит проверка кол-ва фотонов
        if count1==0  % Если 0 фотонов
            iter_0=iter_0+1;
        end
        if count1==1  % Если 1 фотон
            iter_1=iter_1+1;
        end
         if count1==2  % Если 2 фотона
            iter_2=iter_2+1;
         end
         if count1==3   % Если два фотона
            iter_3=iter_3+1;
         end
        count=0;
        count1=0;
    end;
end;
% P’C‹PIPsPґ PSP° CЌPєCЪP°PS
disp('                                  Количество окон
disp(b);
disp('                                  Количество окон с фотонами
```

```
disp(iter_1+iter_2+iter_3-3);

disp('                                  % пустых
pay_0=(iter_0-1)*(1./b)*100;
disp(pay_0);
disp('                                  % однофотонных
pay_1=(iter_1-1)*(1./b)*100;
disp(pay_1);
if (pay_1>7) && (pay_1<11)
    disp('Статистика выполняется')
end;
disp('                                  % двух- и более фотонных посылок');
pay_2=(iter_2+iter_3-2)*(1./b)*100;
disp(pay_2);
if (pay_2>0) && (pay_2<1)
    disp('Статистика выполняется')
end;
hold on;
grid on;
x= [0 1 2];
y= [pay_0/100 pay_1/100 pay_2/100];
plot(x,y,'*','Color',[.1 .7 .7],'LineWidth',3);
% Теоретический
res=0;
alpha=0.1;
for n=0:1:2
    res=( (alpha ^ n) * (exp(-alpha)) ) / factorial(n);
    plot(n,res,'*','Color',[.255 .255 .255],'LineWidth',3);
end;
legend('Experemental data','Theoretical data',1);
```

Количество пустых, одно-, двух- и более фотонных посылок при работе подсистемы статистического контроля без перехвата



Количество пустых, одно-, двух- и более фотонных посылок при работе подсистемы статистического контроля в присутствии перехвата