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»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Томск - 2016

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Томский государственный университет систем управления и радиоэлектроники» (ТУСУР)

Научный руководитель: **Задорин Анатолий Семенович**
доктор физико-математических наук, профессор, заведующий кафедрой радиоэлектроники и защиты информации, ТУСУР, г. Томск

Официальные оппоненты: **Румянцев Константин Евгеньевич**, доктор технических наук, профессор, заведующий кафедрой информационной безопасности телекоммуникационных систем, ФГАОУ ВО «Южный федеральный университет», г. Ростов-на-Дону

Тарасенков Михаил Викторович, кандидат физико-математических наук, старший научный сотрудник лаборатории распространения оптических сигналов, Федеральное государственное бюджетное учреждение науки ИОА СО РАН, г. Томск

Ведущая организация: ФГАОУ ВО «Сибирский федеральный университет», г. Красноярск

Защита состоится «30» июня 2016 г. в 09 час. 00 мин. на заседании диссертационного совета Д212.268.01 на базе ФГБОУ ВПО «Томский государственный университет систем управления и радиоэлектроники» по адресу: 634050, г. Томск, пр. Ленина, 40, ауд. 201.

С диссертацией можно ознакомиться в научной библиотеке ТУСУР по адресу: г. Томск, ул. Красноармейская, 146 и на сайте Томского государственного университета систем управления и радиоэлектроники http://www.tusur.ru/ru/science/education/dissertations/ .

Автореферат разослан «27» мая 2016 г.

Ученый секретарь
диссертационного совета Д212.268.01,
доктор физико-математических наук  А.Е. Мандель

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. 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 и основана на физических законах, в том числе на теореме о запрете клонирования - 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 схемы и модели 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 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 time-bin кубитов, передаваемых по квантовому каналу связи.
4. Предложено использование данных о состоянии кубитов на выходе квантового канала связи 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 режимах 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 time-bin кубитов в системе из нескольких разбалансированных интерферометров Маха-Цендера (ИМЦ).
5. 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 time-bin кубитов позволяет реализовать протокол BB84 в формате временного кодирования.
3. В системах КРК с временным кодированием time-bin 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 time-bin 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.

Апробация результатов работы. Основные результаты диссертационной работы докладывались и обсуждались на следующих конференциях:

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.

Публикации. По результатам исследований опубликованы 13 печатных работ, из которых в рекомендованных ВАК РФ периодических изданиях – 8. Получено свидетельство о государственной регистрации программы для ЭВМ.

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

Структура и объём диссертации. Диссертационная работа состоит из введения, четырех разделов, заключения и 4 приложений. Общий объем диссертации – 132 страницы, в том числе рисунков и схем – 63. Список использованной информации содержит 111 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность темы, определены цель и задачи исследований, представлены научная новизна и практическая значимость работы, изложены положения, выносимые на защиту.

В **первом разделе** рассмотрены основные принципы построения систем квантового распределения ключа. Изложен необходимый для создания формальной модели КРК формализм квантовой механики, в том числе описание состояний отдельных квантовых частиц, а также статистические характеристики ансамблей, представленных фотонами в чистых и смешанных когерентных и фоковских состояниях. Описаны эффекты интерференции амплитуд вероятности этих квантовых частиц, их регистрации и измерение с помощью ИМЦ. Рассмотрено понятие кудита (q-dit), как q-уровневое информационное состояние квантовой частицы, в т.ч. понятие кубита, реализуемое для q=2. Рассмотрены способы приготовления и измерения временных кубитов, они же ТВ-кубиты (time-bin qubits), с помощью ИМЦ.

Дано описание принципов формирования классических протоколов КРК на основе кубитов, приготовленных из одиночных фотонов с поляризационным, фазовым и временным кодированием.

Наиболее подробно рассмотрен предложенный Беннетом и Брассардом протокол BB84.

Механизм защиты основан на случайной смене передающей стороной или пользователем А 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 $\varphi=45^0$ и безошибочное копирование кубитов в данных условиях невозможно. Физическим положением, указывающим на невозможность такого копирования, является теорема о запрете клонирования, которая представляет основание для создания систем КРК всех типов. Указано, что границы применимости данной теоремы для рассмотренных протоколов и модели

квантового канала в виде двоичного симметричного канала без памяти лимитируются максимальной вероятностью ошибок приема битов в канале уровнем p^*.

Отмечается, что если уровень ошибок p в квантовом канале не превышает величину p^*, то детектирование присутствия нелегитимного пользователя в системе может осуществляться, например, за счет контроля уровней коэффициента квантовых ошибок q-BER и B – скорости формирования последовательности $\mathbf{k}_{АБ}$ (битрейт).

Возможность создания нелегитимным пользователем клон-машины для производства копий кубитов последовательности $\mathbf{m}_A$ при этом может быть связана лишь с несовершенством программно-аппаратного устройства системы КРК пользователя А и пользователя Б.

Проанализированы модели расчета помехоустойчивости системы, т.е. величины p. Отмечено, что в квантовом канале, построенном на основе одномодового оптического волокна, уровень системных ошибок p, в основном, определяется приемным оптическим модулем. Рассмотрены соответствующие характеристики фоточувствительных элементов ПрОМ – лавинных фотодиодов (ЛФД), работающие в линейном режиме фоторегистрации, а также фотодиодов специальной конструкции G-SPAD (Single Photon Avalanche Diode), способных работать в ключевом режиме, который в литературе называется гейгеровским.

Описано несколько возможных подходов к созданию клон-машины. В одном из них, основанных на квантовой теории проверки гипотез и оценивания двух неортогональных квантовых состояний с векторами $|\psi_{\pm}\rangle$, вероятность минимальной ошибки в их идентификации определяется границей Хелстрома. В другом способе дискриминации состояний $|\psi_{\pm}\rangle$, так называемом методе обобщенных измерений или UM (unambiguous measurements), результатом является три исхода. Два из них являются корректными, а третий исход с вероятностью $P_?$, характеризует неопределенный результат измерений состояния КЧ. Показано, что достижимый в данном методе обобщенных измерений минимум величины $P_?$, определяется границей Ivanovic-Dieks-Peres (IDP),

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

а сам этот метод служит основой для организации нелегитимным пользователем так называемых UM-атак.

В конце раздела приведены выводы и постановка задачи диссертационного исследования.

Второй раздел диссертации посвящен описанию аппаратной части системы КРК, а также модели ее функциональных характеристик. Здесь дано обобщение модели Персоника помехоустойчивости систем волоконно-оптическими линиями связи на системы КРК с использованием в ПрОМ ЛФД в линейном режиме. Установлена связь схемотехнических решений на уровень ошибок P_f в квантовом канале, вносимых аппаратурой пользователя Б. Показано, что для квантового канала на основе одномодового оптического волокна вероятность P_f связана с q-BER P_q соотношением

$$P_q = P_f + P_E, \qquad (1)$$

где P_E – уровень ошибок, которые вносит нелегитимный пользователь.

При этом скорость B формирования системой «сырого» ключа $\mathbf{k}_{АБ,}$ определяется формулой:

$$B = B_0(1-P_l)\,p(1)k_p 10^{\frac{-(\alpha L)}{10}}, \qquad (2)$$

где B_0 – битовая скорость формирования ключа на стороне А, P_l – вероятность пропуска сигнала, $p(1)$ – априорная вероятность появления фотона при среднем числе фотонов в посылке равном 0,1, L - длина линии связи, α – затухание в ней, k_p –коэффициент, учитывающий протокольное снижение скорости B, для BB84 он составляет 0,5. Результирующая ключевая последовательность $\mathbf{k}_{АБ}^{*}$ в дальнейшем формируется сторонами А и Б в результате применения к «сырому» ключу $\mathbf{k}_{АБ}$ процедуры коррекции ошибок.

Установлено, что при большом уровне коэффициента лавинного размножения ЛФД (M>>1) плотности вероятности $p(n)$ числа n фотоэлектронов в нагрузке ЛФД в отсутствии и присутствии сигнальных фотонов можно считать гауссовыми, так, что:

$$\begin{cases} p(n/u_c=0)=\dfrac{u_0}{\sqrt{2\pi\sigma}}\exp\left(-\dfrac{n^2}{2\sigma^2}\right), \\ p(n/u_c=M)=\dfrac{u_0}{\sqrt{2\pi\sigma}}\exp\left(-\dfrac{(n-M)^2}{2\sigma^2}\right), \end{cases} \qquad (3)$$

где σ - безразмерная шумовая дисперсия:

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

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, C – суммарная емкость выходной цепи ПрОМ, I_2 и I_3 – интегралы Персоника.

Из (3), (4) и классической теории проверки гипотез и оценивания следует, что параметры помехоустойчивости P_l и P_f ПрОМ, находятся как:

$$P_l=\int_{-\infty}^{U_{\text{пор}}} p(n/u_c=0)dn,\quad P_f=\int_{-U_{\text{пор}}}^{\infty} p(n/u_c\neq 0)dn, \qquad (5)$$

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

Отмечается, что особенностью ПрОМ КРК является малость промежутка времени τ, в котором локализованы сигнальные фотоэлектроны, по сравнению с длительностью тактового интервала $T_0 = 1/B_0$. Значение τ определяется уширением импульсной характеристики ЛФД $\delta_c(t)$ τ_0 в тракте ПрОМ в $\zeta = \tau/\tau_0$ раз. Отсюда сделан вывод о том, что свобода в выборе τ и ζ дает возможность оптимизации помехоустойчивости приемника за счет регулировки указанных параметров. График, на рис. 1 показывает пример распределений условных вероятностей

$p(n/u_c)$ в ПрОМ на основе ЛФД Hamamatsu S8664-05K. При этом n – число фотоэлектронов, нормированное относительно отклика фотодиода на один фотон.

Согласно (3), параметры P_l и P_f, находятся путем интегрирования распределений $p(n/u_c = 0)$ и $p(n/u_c = M)$ в пределах, выше и ниже порогового уровня $U_{\text{пор}}$. соответственно.

При анализе данных рис. 1 следует учитывать еще одну особенность систем КРК, отличающую их от ПрОМ, применяемых в оптической связи. Помехоустойчивость последних, как известно, определяется суммой P_l и P_f. Поэтому оптимальным уровнем порога $U_{\text{пор}}$ таких приемников считается точка пересечения кривых $p(n/u_c = 0)$ и $p(n/u_c = M)$ на рис. 1. 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 его генерации (2). По этой причине в системах КРК предлагается устанавливать порог срабатывания решающего устройства $U_{\text{пор}}$ так, чтобы вероятность ложного сигнала P_f не превышала критический уровень, а вероятность пропуска сигнала P_l была минимальной.

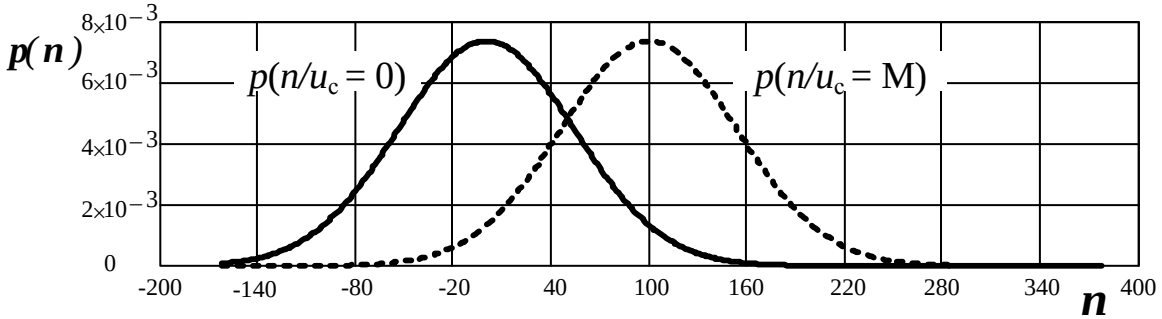

Рис. 1 – Зависимость условных плотностей вероятности числа фотоэлектронов в нагрузке ЛФД S8664-05K, нормированных относительно отклика фотодиода на один фотон, при наличии и отсутствии на входе его оптического порта одиночного фотона

Выполненные расчеты с помощью данной модели помехоустойчивости с использованием в ПрОМ ЛФД Hamamatsu S8664-05K при комнатной температуре показывают возможность реализации системы КРК. При $U_{\text{пор}} = 80$, $P_f = 0{,}07$, длине линии связи 1 км и затухании в оптическом волокне 2 дБ/км скорость генерации ключа будет составлять 10,2 Кб/с.

Используемый в данных расчетах ЛФД Hamamatsu S8664-05K работает в линейном режиме. Соответствующее напряжение питания ЛФД должно быть ~ 400 В и обеспечивать минимальный уровень пульсаций. Нами был разработан такой малогабаритный источник питания.

Для его реализации была выбрана схема повышающего преобразователя на основе микросхемы LM5022, имеющей отдельный выход для управления ключом, роль которого выполняет транзистор VT_1. В схеме предусмотрена обратная связь для стабилизации напряжения, введены два потенциометра для грубой и точной подстройки выходного напряжения.

Разработанный импульсный источник питания обеспечивает выходное напряжение до 500 В и уровень пульсаций, не превышающий 18 мВ.

В качестве фотодиода в ПрОМ систем КРК можно использовать также и ЛФД в гейгеровском режиме (G-SPAD или SPAD), который работает при напряжении выше порогового. Благодаря большому внутреннему усилению, отклик таких диодов на одиночные фотоны может достигать макроуровней, порядка нескольких вольт. На этом фоне внутренние шумы предварительного усилителя ПрОМ оказываются пренебрежительно малыми. Причинами возникновения ошибок P_f в данных условиях являются эффекты афтерпалсинга и самопроизвольного срабатывания устройства при протекании темнового тока. Для снижения влияния указанных эффектов на уровень P_f, необходимо обеспечить работы диода с активным гашением лавины, т.е. импульсный режим, при котором питание на G-SPAD подается в течении короткого времени τ~1нс. 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.

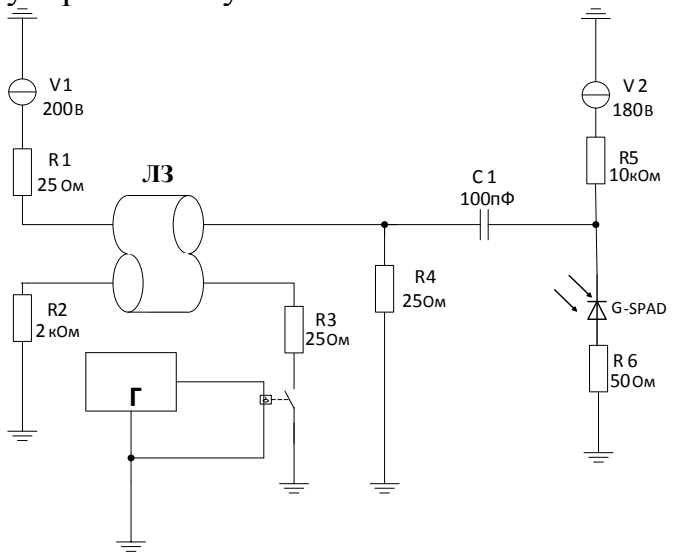

Рис. 2 - Схема формирователя импульсов перенапряжения с разрядной линией

Для решения этой задачи предложено использование формирователя напряжения на разрядных линиях. Принцип работы такого формирователя основан на импульсном преобразовании энергии, накопленной в линии от источника напряжения U_0 при коммутации линии к нагрузке. Длительность импульса $\tau_и$, формируемого на нагрузке, определяется удвоенным временем прохождения электромагнитной волны по отрезку линии задержки.

Предложенная схема формирователя импульсов напряжения исследовалась на компьютерной модели. На рис. 2 приведена исследуемая схема формирователя на разрядной линии, а на рис. 3 – результаты моделирования динамических характеристик формирователя. В качестве диода рассматривается Laser Components G-SPAD SAP500-Series.

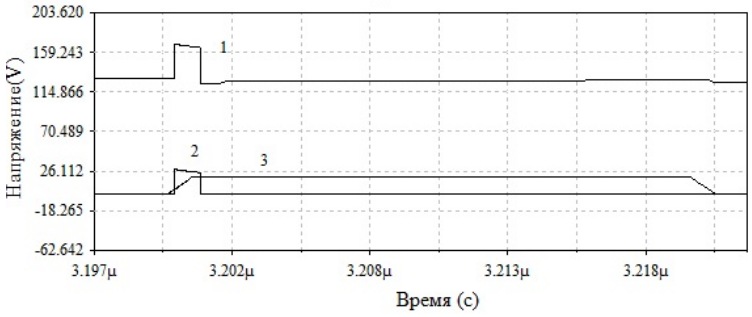

Рис. 3 - Результаты моделирования схемы формирователя стробирующего импульса, 1 – импульс на выходе формирователя, 2 –импульс выходного напряжения фотодиода, 3 – импульс запуска формирователя

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

ЛФД в гейгеровском режиме отличаются лучшей помехоустойчивостью по сравнению с ЛФД в линейном режиме, однако стоят существенно дороже. По этой причине для разработки системы КРК с временным кодированием ориентированной на простоту и доступность рекомендуется использовать ЛФД в линейном режиме.

Для разработки модели трансформации time-bin кубитов необходимо обобщение известной модели симметричного ИМЦ на случай системы из нескольких последовательно включенных разбалансированных интерферометров. С этой целью в структурную схему ИМЦ, помимо вентилей Адамара H и фазовращательных вентилей P, вводится вентиль сдвига D, описывающий относительный временной сдвиг Δ в одном из плеч интерферометра (рис. 4).

В данной схеме преобразование кубита $|\psi_0\rangle$ определяется линейным матричным уравнением:

$$\left|\psi_4\right\rangle = \mathbf{H}\cdot\mathbf{P}\cdot\mathbf{D}\cdot\mathbf{H}\cdot\left|\psi_0\right\rangle \qquad (6)$$

При $|\psi_0\rangle=|0\rangle$ вектор состояния кубита $|\psi_4\rangle$ на выходных портах $|0\rangle$ и $|1\rangle$ ИМЦ определится как:

$$\left|\psi_4\right\rangle = \frac{1}{2}\left[e^{j\alpha_0}D + e^{j\alpha_1}\right]\left|0\right\rangle + \frac{1}{2}\left[e^{j\alpha_0}D - e^{j\alpha_1}\right]\left|1\right\rangle \qquad (7)$$

Формула (7) показывает, что состояние $|\psi_4\rangle$ одиночного фотона в портах $|0\rangle$ и $|1\rangle$ разбалансированного интерферометра представляется time-bin 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. 4. Формальную модель

измерений можно получить путем замены в (7) состояния $|\psi_0\rangle=|0\rangle$ на входе ИМЦ на соотношение (6). При этом следует учесть, что матрицы **P** фазовращающих вентилей интерферометров всегда различны. При расчете кет-вектора $|\psi_4\rangle$ системы из двух ИМЦ следует также учесть фазовую матрицу $\mathbf{P}_{qc}$ квантового канала, в общем случае состоящего из двух оптических волокон, объединяющих соответствующие порты интерферометров.

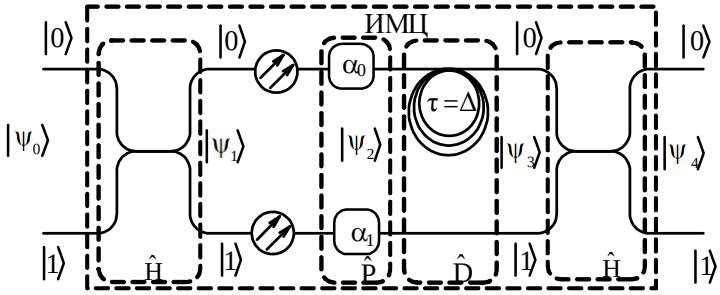

Рис. 4 Структурная схема разбалансированного интерферометра Маха-Цендера

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

$$\left|\psi_4\right\rangle=\frac{1}{2}\mathbf{P}_{qc}\cdot\mathbf{H}_{\text{Б}}\cdot\mathbf{P}_{\text{Б}}\cdot\mathbf{D}\cdot\mathbf{H}_{\text{Б}}\cdot\begin{bmatrix}e^{j\alpha_{\text{A}0}}D_{\text{A}}+e^{j\alpha_{\text{A}1}}\\ e^{j\alpha_{\text{A}0}}D_{\text{A}}-e^{j\alpha_{\text{A}1}}\end{bmatrix}. \tag{8}$$

Соотношение (8) можно применить для анализа системы из двух интерферометров, один из портов которых, $|0\rangle$ или $|1\rangle$, объединены квантовым оптоволоконным каналом:

$$\begin{aligned}\left|\psi_4\right\rangle=&\frac{1}{4}\left[\left(e^{j\alpha_{\text{A}1}}+D_{\text{A}}e^{j\alpha_{\text{A}0}}\right)\left(e^{j\alpha_{qc0}}e^{j\alpha_{\text{Б}1}}+D_{\text{Б}}e^{j\alpha_{\text{Б}0}}e^{j\alpha_{qc0}}\right)\right]|0\rangle-\\&-\frac{1}{4}\left[\left(e^{j\alpha_{\text{A}1}}+D_{\text{A}}e^{j\alpha_{\text{A}0}}\right)\left(e^{j\alpha_{\text{Б}1}}e^{j\alpha_{qc1}}-D_{\text{Б}}e^{j\alpha_{\text{Б}0}}e^{j\alpha_{qc1}}\right)\right]|1\rangle\end{aligned} \tag{9}$$

Заметим, что операторы D_A и $D_Б$ в (9) описывают сдвиги во времени в длинных (Д) плечах ИМЦ-А, Б, а единичный оператор - отсутствие таких сдвигов для коротких (К) плеч интерферометров соответственно. Если $D_A=D_Б$, тогда размерность вектора состояний одиночного фотона на выходных портах второго ИМЦ равна 3, а сам объект $|\psi_4\rangle$ обращается в кутрит. Линейно независимые динамические состояния данного квантового объекта удобно выбрать в качестве базисных векторов, обозначив их как $|\alpha\rangle$, $|\beta\rangle$ и $|\gamma\rangle$. Наиболее интересным информационным состоянием кутрита является состояние $|\beta\rangle$, формирующееся в условиях равенства оптических длин L_1 и L_2 траекторий $Д_A$-$К_Б$ и $К_A$-$Д_Б$, при которых квантовая частица способна интерферировать сама с собой. Результаты этой интерференции проявляются в зависимости амплитуд вероятности $|\beta\rangle$ в выходных оптических портах ИМЦ-Б от разности фаз $\phi=(\alpha_{Б0}+\alpha_{A1})-(\alpha_{Б1}+\alpha_{A0})$ и будут пропорциональны $P_1\sim\cos(\phi/2)$, $P_2\sim\sin(\phi/2)$ соответственно.

Использование одного оптического волокна между ИМЦ-А и ИМЦ-Б характерно для систем с фазовым кодированием квантовых состояний, требующих

точную настройку разности фаз ϕ плеч ИМЦ-А, Б. Такая технология, очевидно, приводит к потерям квантовых частиц в квантовом канале, связанным с отбрасыванием направляемых в волоконный терминатор кубитов из порта $|1\rangle$ ИМЦ-А.

Снижение указанных потерь битрейта можно получить в схеме с временным кодированием кубитов, в которой порты обоих интерферометров соединены оптическими волокнами. Здесь параметр ϕ используется не для кодирования кубитов, а лишь как средство контроля их целостности. Данное обстоятельство позволяет снизить требования к точности балансировки плеч интерферометров и делает возможным использование второго оптического волокна в схеме рис. 4 с целью увеличения системного битрейта в два раза. В данном случае вместо (9) получим:

$$
\begin{aligned}
|\psi_4\rangle = \frac{1}{4}\Big\{&\left(e^{j\alpha_{\text{А}1}} - D_{\text{А}} e^{j\alpha_{\text{А}0}}\right)\left(e^{j\alpha_{\text{Б}1}} e^{j\alpha_{qc0}} - D_{\text{А}} e^{j\alpha_{\text{Б}0}} e^{j\alpha_{qc0}}\right) + \\
&+\left(e^{j\alpha_{\text{А}0}} + D_{\text{А}} e^{j\alpha_{\text{А}0}}\right)\left(e^{j\alpha_{\text{Б}1}} e^{j\alpha_{qc0}} + D_{\text{А}} e^{j\alpha_{\text{Б}0}} e^{j\alpha_{qc0}}\right)\Big\}|0\rangle - \\
&-\frac{1}{4}\Big\{\left(e^{j\alpha_{\text{А}1}} - D_{\text{А}} e^{j\alpha_{\text{А}0}}\right)\left(e^{j\alpha_{\text{Б}1}} e^{j\alpha_{qc1}} + D_{\text{А}} e^{j\alpha_{\text{Б}0}} e^{j\alpha_{qc1}}\right) + \\
&+\left(e^{j\alpha_{\text{А}1}} + D_{\text{А}} e^{j\alpha_{\text{А}0}}\right)\left(e^{j\alpha_{\text{Б}1}} e^{j\alpha_{qc1}} - D_{\text{А}} e^{j\alpha_{\text{Б}0}} e^{j\alpha_{qc1}}\right)\Big\}|1\rangle. \qquad (10)
\end{aligned}
$$

Из (10) видно, что в квантовом канале, построенном из волокон с одинаковыми фазовыми характеристиками структура интерференционной картины зависит от разности фаз $\phi_{qc}=\alpha_{qc0}-\alpha_{qc1}$. Так при $\phi_{qc}=\pi$, согласно (10) условие конструктивной интерференции будет выполняться для состояния $|\beta\rangle$ кутрита, при этом состояния $|\alpha\rangle$ и $|\gamma\rangle$ окажутся подавленными.

Показано, что за счет изменения разности фаз ϕ в плечах ИМЦ-А, Б, а также в волокнах квантового канала можно управлять структурой интерференционной картины в выходных портах ИМЦ-Б.

В **третьей главе** диссертации изложены результаты разработки и исследования модели системы КРК, основанной на методе временного кодирования, предложенном С.Н. Молотковым (M04) и Debuisschert T., Boucher W. (DB04), дополненной подсистемами статистического и интерферометрического контроля.

Логическая схема рассматриваемого здесь протокола приведена на рис. 5, на котором изображен один тактовый интервал, в пределах которого показаны различные возможные временные (кодовые) состояния фотонов, изображенные в виде коротких импульсов. Вертикальной жирной меткой на каждом рисунке обозначены тактовые синхроимпульсы. Символами Б-*i* слева на рис. 5 пронумерованы базисные состояния фотонов, а символами Δ_i снизу отмечены тайм-слоты в пределах каждого из базисов. Из рис. 5 видно, что представленный алгоритм кодирования обеспечивает равную вероятность появления символов «0» и «1» в каждом тайм-слоте тактового интервала.

Соответствующая структурная схема системы дана на рис. 6. Здесь, генераторами псевдослучайных последовательностей ПСП 0–1 и ПСП Δi задаются значения символов коротких импульсов и номер тайм-слота 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 коротких 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 пользователю Б.

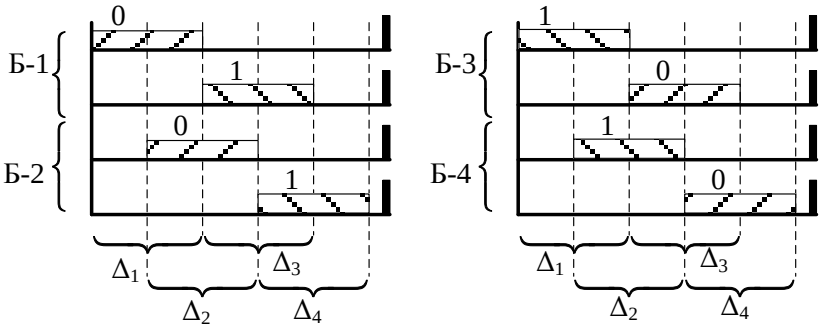

Рис. 5 Кодовые состояния базисов протокола BB84-ВК

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. пользователь Б случайным образом выбирает тайм-слот, в котором его ПрОМ готов к приему очередного одиночного фотона. В соответствии с форматом BB84, пользователь Б по открытому каналу пересылает пользователь А номер использованного для измерения базиса, если фотон оказался продетектирован в указанном тайм-слоте. В случае совпадения Б-*i*, сторона А извещает об этом сторону Б и оба пользователя записывают значения символов из ПСП 0-1 в память в качестве элемента ключевого массива $\mathbf{k}_{АБ}$.

При этом для усиления защищенности канала КРК, сигнализация совпадения базисов организована лишь в конце тактового интервала.

Разработанная модель использовалась нами для измерения вероятности генерации ложных символов P_f ключа в отсутствии и присутствии белых гауссовых шумов.

Обработка данных происходит с помощью подпрограммы, обеспечивающей посимвольную сверку ключевых последовательностей $\mathbf{k}_{АБ}$ на обоих сторонах канала связи и фиксирующей номера тайм-слотов, содержащих ошибочные символы.

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, нормированного к средней амплитуде *a* отклика приемника на пришедший фотон, показаны на рис. 7.

Цифрами *1* и *2* на рис. 7 отмечены кривые $P_f(U_p)$, измеренные при различных среднеквадратичных амплитудах шумового напряжения $U_ш$ на входе компаратора,

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% с помощью регулировки порога U_p.

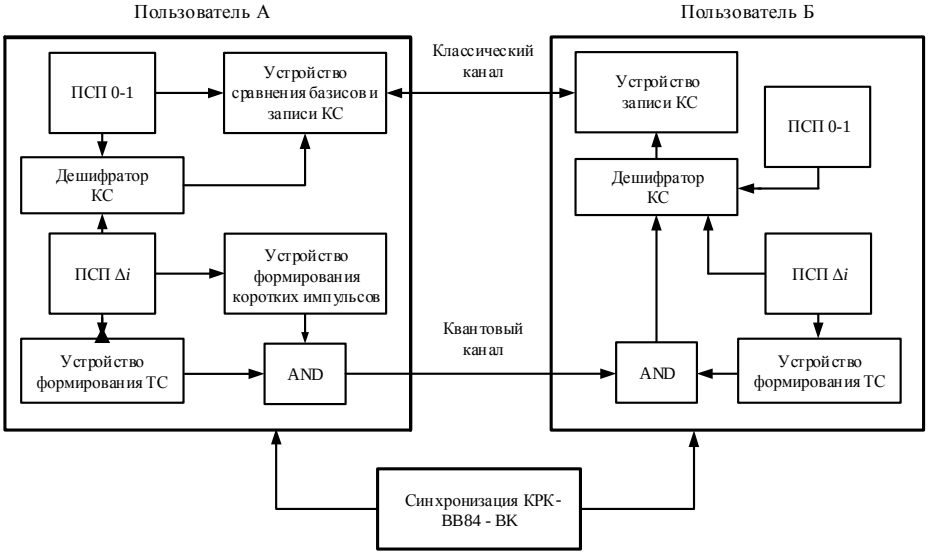

Рис. 6 Структурная схема приемо-передающей части системы КРК-ВК

Показано, 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 ключа (1).

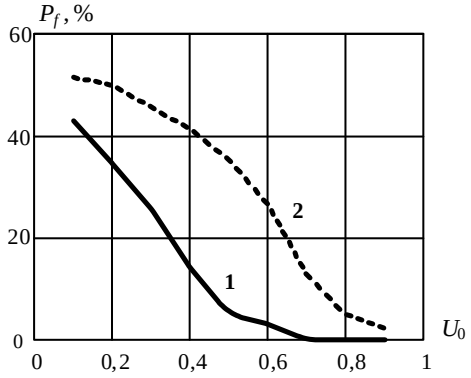

Рис. 7 Доля ложных символов в зависимости от порога компаратора

Отмечается, что измерения состояний квантовых частиц в указанной схеме протокола КРК, фактически, являются проекционными, поскольку исключают неоднозначные оценки временного положения одиночного фотона в квантовом канале, а сам метод кодирования квантовых частиц является одноуровневым.

Данная особенность организации КРК с временным кодированием снижает защищенность системы и требует дополнительных способов защиты протокола.

Показано, что одним из путей решения данной проблемы может являться использование подсистем статистического и интерферометрического контроля состояний, принятых квантовых частиц. В работе предложены варианты возможной программно-аппаратной реализации указанных подсистем.

Для случая использования пользователем А когерентных состояний квантовых частиц с пуассоновской статистикой основой для первой подсистемы служат изменения в статистике распределений вероятностей, вносимых нелегитимным пользователем пустых, одно-, двух- и более фотонных посылок. С этой целью, а также для настройки и отладки системы КРК, в состав разработанной программы введен эмулятор нелегитимного пользователя, имитирующий присутствие клон-машины нелегитимного пользователя в квантовом канале, формирующей когерентные состояния квантовых частиц с заданной статистикой. Для когерентных состояний $|\alpha\rangle$ алгоритм построения клон-машины при этом может быть рассчитан либо на сохранение битрейта кубитов в квантовом канале, либо на сохранении стандартного пуассоновского распределения $p(n)$ числа фотонов n в состояниях $|\alpha\rangle$. В работе показано, что для квантовых частиц в состояниях Глаубера совместить оба условия не представляется возможным.

В качестве примера на рис. 8. приведен расчетный график зависимости битрейта системы КРК, нормированный относительно максимальной битовой скорости генерации ключа в невозмущенном квантовом канале, от процентного состава двух- и более фотонных квантовых состояний $|\alpha_i\rangle$ в последовательности кубитов, передаваемых по квантовому каналу.

Из приведенного графика видно, что реализация первого из указанных выше алгоритмов построения клон-машины приводит к ~9-кратному увеличению доли многофотонных состояний в последовательности $|\alpha_i\rangle$, а второго – к ~10-кратному снижению квантового битрейта. Динамическое измерение указанных параметров и лежит в основе построения подсистемы статистического контроля системы КРК.

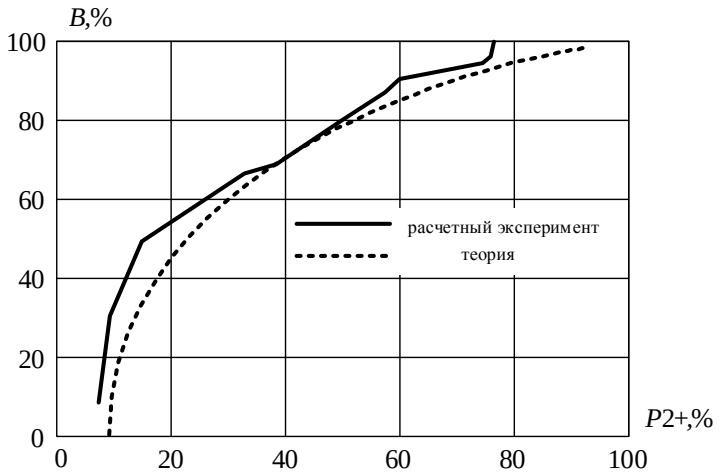

Рис. 8 Теоретическая и экспериментальная зависимости изменения битовой скорости B от процентной доли двух- и более фотонных посылок в условиях присутствия нелегитимного пользователя в квантовом канале

Далее показано, что статистический контроль в квантовом канале не может обеспечить безусловной защищенности канала КРК. Например, применение подсистемы статистического контроля оказывается неэффективным 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 time-bin 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. 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 time-bin кубитов в качестве decoy-states $|\psi^*\rangle$, свободна от указанного недостатка.

Функциональная схема подсистемы интерферометрического контроля, используемая нами для симуляции подсистемы, изображена на рис. 9. Подсистема состоит из устройства случайного выбора траектории квантовой частицы по следующей комбинации плеч ИМЦ-А, Б: 0 – «короткое-короткое», 1 – «длинное-длинное», и 2 – «длинное-короткое» и «короткое-длинное». Настройка распределений вероятностей при этом была следующей: для комбинаций 0 и 1 – по 25%, для 2 – 50%.

На этом рисунке имитирующий квантовую частицу управляющий импульс следует через ИМЦ А и Б по по одной из траекторий 0 или 1, или же сразу по обеим траекториям 2. При этом, вероятности P_1, P_2 зависят от фазового сдвига ϕ, приобретаемого квантовой частицей на указанных траекториях. Устройство распределения на рис. 9 формирует вероятности P_1, P_2 появления квантовой частицы в выходных портах ИМЦ Б в соответствии с формулой (9), т.е. в зависимости от фазового сдвига $\Delta\phi$. Указанные последовательности квантовых частиц далее регистрируется двумя пороговыми ПрОМ-1,2 по частоте

срабатывания которых дается оценка P_1 и P_2. В рассматриваемом протоколе в большинстве тактовых интервалов фрейма используются простые, одноуровневые квантовые состояния, обеспечивающие $P_1 \approx P_2$.

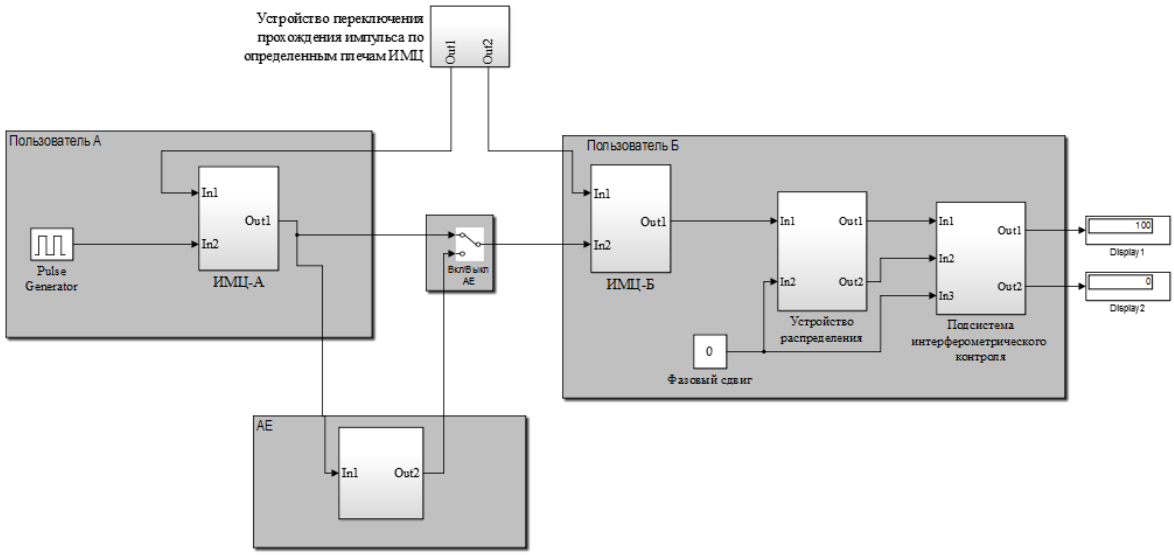

Рис. 9 Функциональная схема подсистемы интерферометрического контроля

Нарушение указанного равенства происходит лишь в некоторых, случайно выбранных пользователем А тайм-слотах фрейма, снабженных проверочными DS-кубитами $|\psi^*\rangle$. Случайный характер позиций $|\psi^*\rangle$ не дает возможности нелегитимному пользователю своевременного переключения режимов обработки его клон-машиной одно- или двухуровневых состояний квантовых частиц в квантовом канале. Уровень соответствующих ошибок при этом позволяет детектировать работу клон-машины.

В качестве примера на рис. 10 представлены результаты моделирования работы подсистемы интерферометрического контроля по схеме рис. 9, на которых показана доля срабатываний ПрОМ-1 в присутствии n_{fd1E} и отсутствии n_{fd1} нелегитимного пользователя в зависимости от фазового сдвига $\Delta\phi$.

В работе отмечено, что для проявления интерференционной картины амплитуд вероятностей квантовых частиц, подобной изображенной на рис. 10, необходимо проведение серии из N измерений. При этом показано, что в приближении гауссовой статистики $|\psi^*\rangle$ возможность дискриминации состояний квантовых частиц по значению $\Delta\phi$ для N измерений с заданной доверительной вероятностью p_c, может может быть установлена на основе статистики Стьюдента. В частности показано, что при p_c=0,95 минимальное число измерений $N^* \geq 4$.

Если каждый фрейм содержит по только один защитный DS-кубит, то с учетом снижения битрейта в квантовом канале, описываемого коэффициентом $\zeta = B/B_0$ в формуле (2), среднее число фреймов, необходимых для реализации измерений будет равно N^*/ζ. Приведенная оценка позволяет выразить минимальное время T^* детектирования работы клон-машины через длительность фрейма T, коэффициент лавинного размножения M и пороговый уровень ПрОМ, а также потери квантовых частиц в квантовом канале как $T^* = T \cdot N^*/\zeta(\alpha L, M, U_{пор})$. Например для

рассмотренного выше ПрОМ с ЛФД Hamamatsu S8664-05K с характеристиками, указанными в комментариях к рис. 1, и $T\approx10^{-3}$с., $T^{*}\approx2$с. С помощью приведенных оценок показано, что снижение T^{*} может осуществляться за счет увеличения числа проверочных вставок DS-кубитов во фрейм.

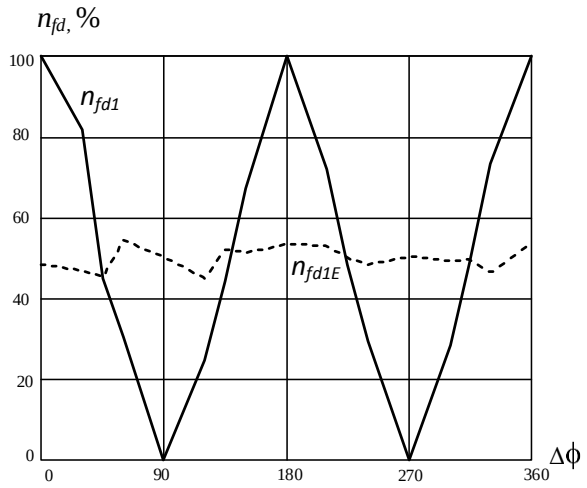

Рис. 10 Доля срабатываний ПрОМ-1 в присутствии и отсутствии нелегитимного пользователя

Четвертая глава посвящена разработке и исследованию оптоволоконной системы КРК, работающей по протоколу BB84 с кодированием квантовых частиц двухуровневыми динамическими состояниями. Ниже он обозначен как BB84 с временным кодированием. Здесь, в отличие от классического протокола, поляризационные кубиты с малым временем декогеренции заменены кубитами, вычислительный базис которых, задан одно-, или двукратными временными сдвигами состояния $|\psi_0\rangle$ одиночного фотона в ИМЦ, так, что,

$$|\psi_1\rangle=\mathbf{D}|\psi_0\rangle, \qquad |\psi_2\rangle=\mathbf{D}|\psi_1\rangle, \tag{11}$$

где D - оператор сдвига на время Δ, $|\psi_0\rangle$ - кет-вектор исходного одноуровневого состояния.

Указанные квантовые частицы в литературе трактуется как time-bin кубиты. Такие квантовые объекты обеспечивают наибольшую устойчивость однофотонных состояний к динамическим флуктуациям параметров оптоволоконного квантового канала связи и являются основой метода временного кодирования, при котором кодовое состояние (0 или 1) $|\psi_2\rangle$ определяется их положением относительно границ заданных временных промежутков тактового интервала.

Замена всей последовательности одноуровневых когерентных состояний $|\alpha_i\rangle$ фрейма на устойчивые при распространении по оптическому волокну time-bin кубиты позволяет достичь стандартного уровня защищенности протокола BB84. В частности, среднее время детектирования клон-машиной T^{*} в данной системе снижается в тысячи раз, прямо пропорционально числу тактовых интервалов в системном фрейме.

В главе детально описаны логический и физический уровни реализации предложенного протокола BB84 с временным кодированием. Рассмотрены

процессы приготовления и детектирования временных кубитов в системе из двух идентичных, разбалансированных ИМЦ. На рисунке 11 показаны два используемых для этой цели вычислительных базиса. Первый из них, **I** построен на кет-векторах $|\psi_{02}\rangle$, $|\psi_{22}\rangle$, а второй – **II**, на $|\psi_{32}\rangle$, $|\psi_{12}\rangle$. Здесь соответствие заштрихованных временных интервалов (тайм-слотов), в которых может быть локализована квантовая частица в результате измерения, и кодовых символов 0 и 1, помечено стрелкой →. Индекс m в $|\psi_{mn}\rangle$ указывает на номер одной из четырех возможных векторных комбинаций, а n – число состояний. Из рис. 11 видно, что в рассматриваемой здесь схеме КРК на выходе ИМЦ-А приготавливаются только двухуровневые (n=2) состояния фотонов – time-bin кубиты $|\psi_{m2}\rangle$. После обработки $|\psi_{m2}\rangle$ на приемной стороне, в ИМЦ-Б, формируются еще один - третий возможный уровень квантовых частиц, выделенный на рис. 11 пунктирной линией. Такая квантовая частица называется кутритом $|\psi_{m3}\rangle$, представленным в плечах ИМЦ-Б двумя состояниями, обозначенными на функциональной схеме системы (рис. 12) как $|\psi_{m3,1}\rangle$ и $|\psi_{m3,2}\rangle$. Из рис. 11 видно, что однозначная связь $|\psi_{m3}\rangle$ с переносимым ею кодовым символом имеет место лишь для информационного состояния кутрита $|1_m\rangle$, локализованного в (m+1) тайм-слоте тактового интервала. В указанном состоянии проявляется интерференция амплитуд вероятностей time-bin кубитов, позволяющая сторонам А и Б контролировать целостность кубитов $|\psi_{m2}\rangle$ при их передаче по квантовому каналу. Остальные состояния $|0_m\rangle$ и $|2_m\rangle$ принятых стороной Б кутритов $|\psi_{m3,1}\rangle$ и $|\psi_{m3,2}\rangle$ отбрасываться при формировании $\mathbf{k}_{АБ}$.

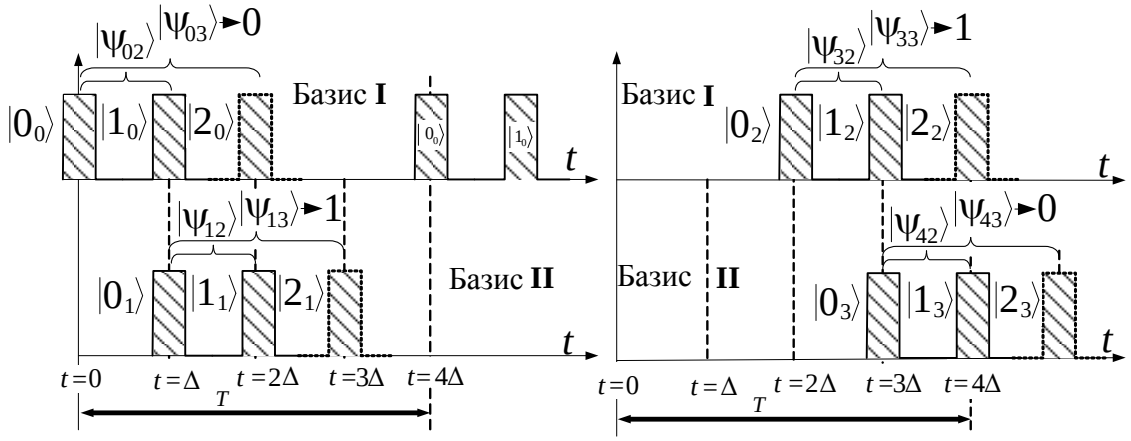

Рис. 11 - Связь четырех сдвинутых во времени состояний time-bin кубитов $|\psi_{m2}\rangle$ и кутритов $|\psi_{m3}\rangle$ с базисами I и II и кодовыми символами 0 и 1 на тактовом интервале

Передача в предложенной схеме КРК по квантовому каналу квантовых частиц в формате кубитов $|\psi_{m2}\rangle$ означает равную вероятность локализации $|\psi_{m2}\rangle$ в двух смежных тайм-слотах: m-м и m+1-м (рис. 11). Показано, что в данных условиях ортогональные базисы **I** и **II,** развернуты друг относительно друга на 45 градусов, поэтому попытки клонирования $\mathbf{m}_A$ всегда всегда связаны с необходимостью принятия решений о базисе, в котором был приготовлен каждый кубит. Уровень неизбежных при этом ошибок контролируется пользователем А и пользователем Б

в рамках стандартных протокольных переговоров по классическому каналу, а присутствие клон-машины в квантовом канале устанавливается по генерации избыточных ошибок в выборе базиса.

Отмечается, что основной объем информации об указанных ошибках содержится в отбрасываемых сведениях о состояниях кутритов $|\psi_{m3}\rangle$ в тактах последовательности $\mathbf{m}_A$, где состояния базисов пользователя А и пользователя Б не совпали. Для повышения защищенности системы в работе предлагается обмен указанной информацией между легитимными пользователями по классическому каналу.

Организация контроля целостности time-bin кубитов $|\psi_{m2}\rangle$ в протоколе BB84 с временным кодированием обеспечивается подсистемой интерференционного контроля, аналогично тому, как это было сделано в описанном в 3 главе DS-протоколе КРК, где time-bin кубиты применялись в качестве проверочных DS-кубитов $|\psi^*\rangle$. Однако в рассматриваемом протоколе такая проверка проводится в каждом тактовом интервале фрейма *T*, т.е. в тысячи раз чаще.

Показано, что дополнительной формой проверки целостности объектов $|\psi_{m2}\rangle$ является контроль статистики распределения стояний $|0_m\rangle$, $|1_m\rangle$ и $|2_m\rangle$ кутрита $|\psi_{m3}\rangle$ при преобразовании $|\psi_{m2}\rangle$ в $|\psi_{m3}\rangle$ в ИМЦ-Б. Контроль основан на неопределенности в выборе базиса при подмене $|\psi_{m2}\rangle$ в клон-машине нелегитимного пользователя, которая приводит к вероятности регистрации фотонов не только в *m*-м, *m*+1-м и *m*+2-м тайм-слотах тактового интервала, но также и в (*m*-1)-м, (*m*+2)-м и (*m*+3)-м тайм-слотах. При этом соответствующие вероятности будут: 0.25, 0.5, 0.25 и ~ 0.083, 0.25, 0.33, 0.25 и 0.083. Контроль указанных распределений и позволяет дополнительно усилить защищенность рассматриваемого протокола BB84 с временным кодированием.

В качестве прототипа программно-аппаратной реализации описанного выше протокола нами рассматривалась приведенная на рис. 12 структурная схема системы КРК.

В этой схеме одиночный фотон в одноуровневом глауберовском состоянии $|\psi_0\rangle$ приготавливается путем стробирования лазерного излучения передающего оптического модуля (ПОМ) электрооптическим модулятором (ЭОМ) с последующим необходимым ослаблением $|\psi_0\rangle$ в оптическом аттенюаторе.

Локализация $|\psi_0\rangle$ в тайм-слоте тактового интервала, с кодовым состоянием, соответствующим той или иной комбинации на рис. 11, осуществляется за счет сдвига управляющего сигнала ЭОМ на время t=0, Δ, 2Δ или 3Δ. time-bin кубиты формируются в расположенном далее ИМЦ-А. Сформированная таким образом последовательность $\mathbf{m}_A$ с выхода интерферометра направляется в квантовый канал.

В интерферометре ИМЦ-Б временные кубиты $\mathbf{m}_A$ преобразуется в две последовательности кутритов $|\psi_{m31}\rangle$ и $|\psi_{m32}\rangle$ регистрируемых приемными оптическими модулями ПрОМ-1,2 на стороне Б. Комплексные амплитуды вероятностей $|\psi_{m31}\rangle$ и $|\psi_{m32}\rangle$ определяют вероятности срабатывания детекторов ПрОМ-1,2, а также обеспечивают контроль когерентности кубитов, прошедшим по альтернативным траекториям оптических трактов интерферометров. Как

отмечалось выше, данный контроль позволяет детектировать подмены time-bin кубитов $|\psi_{m2}\rangle$ клон-машиной нелегитимного пользователя простым одноуровневым состоянием $|\psi_0\rangle$. Клонирование же целых кубитов из $\mathbf{m}_A$ детектируются на логическом уровне рассматриваемого протокола BB84 с временным кодированием.

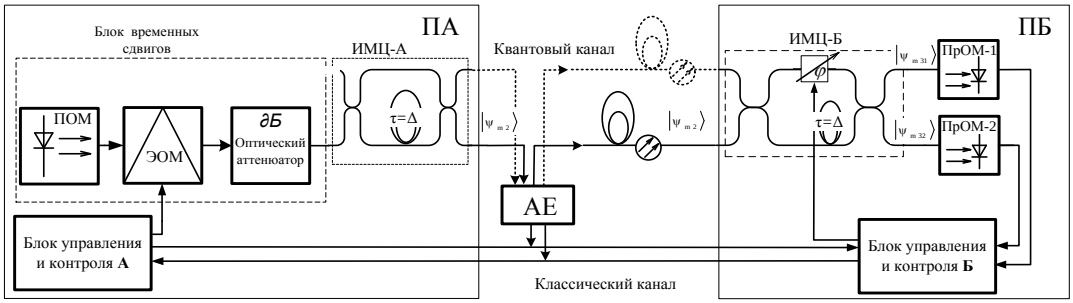

Рис. 12 - Функциональная схема аппаратной части системы КРК с временными сдвигами time-bin кубитов

Для упрощения процедуры контроля, балансировки интерферометров, а также совмещения интерференционного максимума с одним из фотоприемников ПрОМ, в ИМЦ-Б введен фазовращающий вентиль, контролирующий фазовый сдвиг ϕ кубитов на различных траекториях ИМЦ-А, Б. В качестве такого вентиля, например, предлагается использовать дополнительное оптическое волокно, соединяющее вторые плечи ИМЦ-А, Б и позволяющее вдвое увеличить битрейт $\mathbf{k}_{АБ}$ предложенной схемы КРК с временным кодированием.

Проведенные на данной основе исследования различных моделей взаимодействия пользователей А и Б в условиях присутствия нелегитимного пользователя в квантовом канале подтвердили общую функциональность системы. Вместе с тем, полученные результаты представляют решение лишь отдельные части весьма сложной проблемы. Актуальными остаются задачи по исследованию границ защищенности данной системы в реальных условиях.

Заключение. Основными результатами работы являются:

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 ТВ-кубитов по тайм-слотам в пределах тактового интервала. Предложено использование данных о состояниях кубитов, не прошедших протокольную процедуру согласования базисов, для усиления защищенности системы.

Основные результаты диссертационного исследования изложены в следующих работах:

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. 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.
9. 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.
10. 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.
11. Задорин А.С., Махорин Д.А. Временное кодирование состояний фотонов в системе квантового распределения ключей с временным кодированием ТВ-кубитов // Материалы докладов XI Международной научно-практической конференции «Электронные средства и системы управления - 2015», г. Томск, 25-27 ноября 2015г. Часть. 1. С. 265-269.
12. 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 - 2015», г. Томск, 25-27 ноября 2015г. Часть. 1. С. 270-273.
13. Задорин А.С., Махорин Д.А. Принцип квантового распределения ключей по оптическому волокну на основе временных сдвигов ТВ-кубитов // Изв. вузов. Физика. – 2016. – Т.69, №3. – С. 24-29.

Также получено свидетельство о регистрации программы для ЭВМ:

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.