УДК 539.182
ББК 22.314
ГРНТИ 29.31.17
ВАК 01.04.15

Разработка элементов дистанционного курса по физическим основам квантовой криптографии

Я. С. Замлелова [1]

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ульяновский государственный педагогический университет имени И. Н. Ульянова», 432071, Ульяновск, Россия

Поступила в редакцию 18 марта 2021 года
После переработки 14 апреля 2021 года
Опубликована 12 июня 2021 года

Аннотация. Произведено описание разработки элементов онлайн-курса по физическим основам квантовой криптографии при помощи инструментария MOODLE. Онлайн-курс по элементарной физике, созданный при помощи инструментария MOODLE, можно использовать для информационного обеспечения смешанного обучения студентов при изучении физических основ квантовой криптографии, а также для визуализации процесса обучения физическим основам квантовой криптографии. Использование элементов контроля курса по физическим основам квантовой криптографии позволит систематизировать контроль теоретических знаний по физическим основам квантовой криптографии.

Ключевые слова: курс, квантовая криптография, физические основы квантовой криптографии, педагогическое образование, информатизация образования, образовательный процесс университета, методика дистанционного обучения

PACS: 03.67.Dd

Введение

Современное общество характеризуется высокой степенью распространения информационных технологий. Однако с быстрым развитием телекоммуникационных технологий очень остро встаёт вопрос о сохранности с их помощью передаваемых данных. Способам передачи информации по различным каналам связи и методам защиты информации отводится всё более важная роль как в научных исследованиях, так и в повседневной практической деятельности. В конечном итоге сформировалась такая отрасль, как информационная безопасность, и наиболее широкое распространение получает такая наука, как криптография.

Актуальность изучения данной проблемы обусловлена тем, что использование электронных курсов решает проблему систематизации теоретического материала, задач и

[1] E-mail: zamlelowa1998@mail.ru

заданий, а также обеспечивает планомерную выдачу заданий, последовательный контроль и даёт рациональный подход в преподавании курса по физическим основам квантовой криптографии.

Целью исследования является разработка дистанционного курса по физическим основам квантовой криптографии.

В задачи исследования входит анализ научной литературы по квантовой криптографии и разработка дистанционного курса по физическим основам квантовой криптографии.

Объектом исследования является дистанционный курс по физическим основам квантовой криптографии.

Предметом исследования является процесс создания дистанционного курса по физическим основам квантовой криптографии в системе управления обучением MOODLE.

Гипотеза исследования состоит в выяснении того, каковы особенности проектирования дистанционного образовательного ресурса по физическим основам квантовой криптографии.

Создание дистанционного курса по физическим основам квантовой криптографии позволит повысить эффективность самостоятельной работы обучающихся при изучении квантовой криптографии.

В качестве методов исследования используются компьютерные методы создания курсов на платформе MOODLE.

Научная новизна работы заключается в сочетании традиционных и дистанционных технологий при изучении физических основ квантовой криптографии в педагогическом университете.

Материалами исследования являются теоретические материалы курса по физическим основам квантовой криптографии.

Обзор работ по квантовой криптографии и квантовым криптосистемам

Квантовая криптография, или, точнее, распространение квантового ключа, за которым следует одноразовый блокнот, является единственным безопасным способом передачи секретной информации (см. [1] для обзора). Его безопасность основана не на некоторых математических предположениях, таких как вычислительная мощность ограниченного прослушивателя, а на законах квантовой механики. Из-за принципа неопределённости Гейзенберга измерение в квантовой системе изменяет саму систему. Таким образом, измерение Евы в квантовом состоянии, несущем информацию отправителя, приводит к изменению состояния, которое может заметить Алиса и Боб. Безопасность схем распределения квантовых ключей также может быть понята в терминах теоремы отсутствия клонирования [2]. Ева не может сделать и сохранить идеальную копию квантового состояния, несущего информацию от Алисы Бобу. Хорошо известно, что существование совершенной квантовой клонирующей машины позволило бы победить принцип неопределённости Гейзенберга.

Квантовая криптография ещё не вышла на уровень практического использования, но приблизилась к нему. В мире существует несколько организаций, где ведутся активные исследования в области квантовой криптографии. Среди них IBM, GAP-Optique, Mitsubishi, Toshiba, Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт (Caltech), а также молодая компания MagiQ и холдинг QinetiQ, поддерживаемый британским министерством обороны. Диапазон участников охватывает как крупнейшие мировые институты, так и небольшие начинающие компании, что позволяет говорить о начальном периоде в формировании рыночного сегмента, когда в нём на равных могут участвовать и те, и другие.

В настоящее время средства и методы криптографии используются для обеспечения информационной безопасности не только государства, но и частных лиц, организаций. В современный век информационных технологий большой обмен информацией происходит в цифровом виде через открытые каналы связи. Информация может быть повергнута различного рода угрозам: недружественному ознакомлению, подмене, фальсификации, накоплению и т.д. Именно криптография даёт наиболее надёжные методы защиты от таких угроз.

Современные квантовые системы связи основаны на использовании квантовых свойств носителей информации [3]. Если в обычных телекоммуникационных сетях данные кодируются в амплитуде и частоте излучения или электрических колебаний, то в квантовых — в амплитуде электромагнитного поля или в поляризации фотонов [4]. Разумеется, потребуется значительно более дорогая и сложная аппаратура, но эти ухищрения оправданны: дело в том, что передача информации по квантовым каналам обеспечивает стопроцентную защиту от прослушивания. Согласно законам квантовой механики измерение свойств того или иного квантового объекта, например измерение поляризации фотона, неминуемо меняет его состояние. Получатель увидит, что состояние фотонов изменилось, и предотвратить это нельзя в принципе — таковы фундаментальные законы природы.

Конечно же, квантовое направление криптографической защиты информации очень перспективно [5], так как квантовые законы позволяют вывести методы защиты информации на качественно новый уровень. На сегодняшний день уже существует опыт по созданию и апробированию компьютерной сети, защищенной квантово-криптографическими методами — единственной в мире сети, которую невозможно взломать.

В работе [6] рассмотрены две квантовые криптографические схемы, основанные на кодировании ключа в кубитах, то есть в квантовых состояниях в d-мерном гильбертовом пространстве. Первая криптосистема использует две взаимно несмещенные базы (тем самым расширяя схему BB84), в то время как вторая использует все доступные $d + 1$ взаимно несмещенные базы (расширяя протокол шести состояний для кубитов). Затем извлекаем информацию, полученную потенциальным перехватчиком, применяя клонированную индивидуальную атаку, а также верхнюю границу частоты ошибок, которая обеспечивает безусловную защиту от когерентных атак.

В работе [7] проанализировано расстояние распространения секретного ключа в случае строго однофотонного источника для протоколов BB84 и фазового кодирования (протокол PTC).

В работе [8] проанализированы потери, существующие в канале связи, и возможные атаки с однозначными измерениями, приводящие к потере безопасности с учётом того, что источник квантовых состояний не является строго однофотонным. Проблема стабильности протоколов квантового распределения ключей в канале с большими потерями ещё не решена.

В работе [9] предложена новая релятивистская квантовая криптосистема, в которой информация передаётся расширенными однофотонными состояниями с ортогональной поляризацией и эффективной длиной, превышающей длину канала связи. Эффект лёгкого «ареста» используется в качестве процедуры для обнаружения и подготовки расширенных состояний. Криптосистема защищена от попыток подслушивания, поскольку её состояния квантуются, а скорость распространения ограничена. В этой схеме процедуры подготовки и обнаружения являются локальными в пространстве, но требуют конечного времени, в зависимости от расширения состояний. Подготовка к обнаружению в конце приёмника начинается до того, как состояние покинет источник на входе.

В работе [10] показано, что релятивистская квантовая криптография включает в себя не только геометрические свойства векторов состояния квантовой системы в гиль-

бертовом пространстве, но и свойства носителей квантовых состояний в пространстве–времени Минковского. Физический тип квантового объекта, несущего квантовую информацию с чрезвычайно высокой скоростью в пространстве-времени, имеет фундаментальное значение в современной теории квантовой информации.

Структура четырёхмерного пространства-времени Минковского или неприводимые представления группы Пуанкаре в гильбертовом пространстве, ответственна за существование безмассовых частиц, фотонов. В этом смысле структура пространства–времени на самом деле используется в релятивистских системах квантовой криптографии для распределения криптографических ключей. Это позволяет гарантировать безопасность ключей даже при использовании ортогональных состояний.

Рассмотрим работы по безопасности криптографических ключей в системах квантовой криптографии. В работе [11] рассматривается безопасность криптографических ключей в системах квантовой криптографии, которая гарантируется фундаментальными квантово-механическими принципами. Квантовый канал, через который передаются квантовые состояния, не контролируется, и подслушивающее устройство может выполнять с ним любые модификации.

В работе [12] рассматривается безопасность ключей в квантовой криптографии, основанная на фундаментальных квантово-механических исключениях (исключение клонирования и копирования неортогональных квантовых состояний). Физический тип квантового объекта, несущего информацию (фотон, электрон, атом и т. д.) незначителен, важен только его вектор состояния. В релятивистской квантовой криптографии для открытого пространства фундаментальное значение имеют как время информационного носителя (фотон, который распространяется с предельно допустимой скоростью в вакууме), так и его квантовое состояние. Основные фундаментальные ограничения, которые диктуются как специальной теорией относительности, так и квантовой механикой при распознавании неортогональных квантовых состояний позволяют сформулировать принципиально новые протоколы распределения ключей, которые устойчивы к любым атакам на ключ и гарантируют безопасность ключей для нестрого однофотонного источника и исключают любые потери. В связи с этим протокол является протоколом реального времени в пространстве–времени Минковского. Здесь атака на канал связи обнаруживается задержкой результатов измерения подслушивания, протокол не требует синхронизации часов на стороне передатчика и приёмника.

В работе [7] проанализировано расстояние распространения секретного ключа в случае строго однофотонного источника для протоколов BB84 и фазового кодирования (протокол PTC). В работе [8] проанализированы потери, существующие в канале связи, и возможные атаки с однозначными измерениями, приводящие к потере безопасности с учётом того, что источник квантовых состояний не является строго однофотонным. Проблема стабильности протоколов квантового распределения ключей в канале с большими потерями ещё не решена.

В работе [13] предложен новый протокол для квантовой криптографии. Протокол основан на использовании набора измерений, которые позволяют полностью восстановить матрицу плотности, являющуюся носителем информации о физической системе. Такой протокол может быть реализован посредством гомодинного детектирования (хорошо известного в квантовой оптике) электромагнитного поля. В работе [13] приводится пример квантовой криптосистемы, в которой вакуумное состояние фотонного поля используется как одно из двух информационных состояний. Это новейшая методика, которая может быть использована для обеспечения конфиденциальности информации, передаваемой между двумя сторонами, обычно называемой Алисой и Бобом, путём использования противоинтуитивного поведения элементарных частиц, таких как фотоны.

В работе [9] предложена новая релятивистская квантовая криптосистема, в которой

информация передаётся расширенными однофотонными состояниями с ортогональной поляризацией и эффективной длиной, превышающей длину канала связи. Эффект лёгкого «ареста» используется в качестве процедуры для обнаружения и подготовки расширенных состояний. Криптосистема защищена от попыток подслушивания, поскольку её состояния квантуются, а скорость распространения ограничена. В этой схеме процедуры подготовки и обнаружения являются локальными в пространстве, но требуют конечного времени, в зависимости от расширения состояний. Подготовка к обнаружению в конце приёмника начинается до того, как состояние покинет источник на входе.

В работе [10] показано, что релятивистская квантовая криптография включает в себя не только геометрические свойства векторов состояния квантовой системы в гильбертовом пространстве, но и свойства носителей квантовых состояний в пространстве–времени Минковского. Физический тип квантового объекта, несущего квантовую информацию с чрезвычайно высокой скоростью в пространстве-времени, имеет фундаментальное значение.

Структура пространства-времени Минковского или неприводимые представления группы Пуанкаре в гильбертовом пространстве, ответственна за существование безмассовых частиц, фотонов. В этом смысле структура пространства-времени на самом деле используется в релятивистских системах квантовой криптографии для распределения криптографических ключей. Это позволяет гарантировать безопасность ключей даже при использовании ортогональных состояний.

В работе [12] рассматривается безопасность ключей в квантовой криптографии, основанная на фундаментальных квантово-механических исключениях (исключение клонирования и копирования неортогональных квантовых состояний). Физический тип квантового объекта, несущего информацию (фотон, электрон, атом и т. д.) незначителен, важен только его вектор состояния. В релятивистской квантовой криптографии для открытого пространства фундаментальное значение имеют как время информационного носителя (фотон, который распространяется с предельно допустимой скоростью в вакууме), так и его квантовое состояние. Основные фундаментальные ограничения, которые диктуются как специальной теорией относительности, так и квантовой механикой при распознавании неортогональных квантовых состояний позволяют сформулировать принципиально новые протоколы распределения ключей, которые устойчивы к любым атакам на ключ и гарантируют безопасность ключей для нестрого однофотонного источника и исключают любые потери. В связи с этим протокол является протоколом реального времени в пространстве–времени Минковского. Здесь атака на канал связи обнаруживается задержкой результатов измерения подслушивания, протокол не требует синхронизации часов на стороне передатчика и приёмника.

В работе [11] рассматривается безопасность криптографических ключей в системах квантовой криптографии, которая гарантируется фундаментальными квантово-механическими принципами. Квантовый канал, через который передаются квантовые состояния, не контролируется, и подслушивающее устройство может выполнять с ним любые модификации.

В работе [13] предложен новый протокол для квантовой криптографии. Протокол основан на использовании набора измерений, которые позволяют полностью восстановить матрицу плотности, являющуюся носителем информации о физической системе. Такой протокол может быть реализован посредством гомодинного детектирования (хорошо известного в квантовой оптике) электромагнитного поля. В работе [13] приводится пример квантовой криптосистемы, в которой вакуумное состояние фотонного поля используется как одно из двух информационных состояний.

Ограничение на длину линии связи связано с так называемой атакой с расщеплением числа фотонов [14]. Применительно к одному из основных протоколов распределения

ключей BB84 [15] атака с расщеплением числа фотонов сводится к следующему [16]. Подслушиватель (Ева) определяет неразрушающим образом число фотонов в каждой посылке, но не их состояние. На такие измерения не существует принципиальных запретов в квантовой механике. Если обнаружен один фотон, то посылка блокируется. Если обнаружено два и более фотонов, то один из фотонов Ева направляет через свой канал с меньшим затуханием (в идеале без затухания) на приёмную сторону к Бобу, а остальные сохраняет в квантовой памяти и ждет стадии раскрытия базисов. При длине линии выше критической,соответственно потерях в линии, Ева может блокировать все однофотонные посылки, производит ошибки на приёмной стороне, и остаться незамеченной. После раскрытия базисов Ева измеряет состояния в своей квантовой памяти уже в известном базисе. Поскольку в каждом базисе в протоколе BB84 состояния ортогональны, то при известном базисе Ева достоверно узнает каждый передаваемый бит и не производит ошибок на приёмной стороне. Таким образом, для достоверного знания каждого бита ключа Еве достаточно двухфотонной компоненты. Критическая длина линии связи, до которой можно передавать ключи, фактически определяется из того условия, что вероятность потери фотона в линии равна вероятности (доле) однофотонной компоненты в передаваемых квантовых состояниях.

Атака с расщеплением числа фотонов — атака не меняет общего числа посылок, достигающих приёмной стороны, но меняет распределение вероятностей по числам заполнения фотонов. Существующие на сегодняшний день лавинные фотодетекторы не различают числа фотонов, поэтому для обнаружения изменения распределения по числу фотонов требуется существенная модификация как протокола передачи ключей, так и самой системы.

Второй путь нейтрализации атаки с расщеплением числа фотонов — атаки состоит в использовании протоколов, стойких относительно такой атаки. Слабость протокола BB84 относительно атаки с расщеплением числа фотонов, как видно из рассуждений, приведенных выше, состоит в том, что состояния внутри каждого базиса ортогональны. Поэтому естественный способ видоизменения протокола состоит в том, чтобы сделать состояния внутри базисов неортогональными, соответственно, достоверно неразличимыми. Оказывается, что в этом случае для достоверного знания каждого бита Еве достаточно трёхфотонной компоненты. Поэтому протокол секретен до тех пор, пока длина канала связи и потери в нем не превышают такой величины, что Ева может блокировать все одно- и двухфотонные посылки. В полном объёме стойкость подобного протокола не проанализирована [7, 17, 18].

Протокол распределения ключей с фазово-временным кодированием для однофотонного источника не требует сколько-нибудь заметной модификации самой системы и имеет наибольшую критическую ошибку, до которой можно передавать ключи в однофотонном режиме. Был сделан анализ стойкости данного протокола для случая, когда квантовые состояния не являются строго однофотонными, а представляют собой ослабленное лазерное излучение. Оказывается, что для получения достоверной информации о каждом бите ключа Еве необходима, как минимум, пятифотонная компонента. Поэтому длина линии связи и потери должны быть таковы, чтобы Ева могла блокировать все одно-, двух-, трёх-, четырёх- и почти все пятифотонные посылки, чтобы знать каждый бит ключа достоверно. Однако при учёте темновых отсчётов фотодетекторов на приёмной стороне оказывается, что Ева не имеет возможности для атаки с расщеплением числа фотонов, поскольку для данного протокола длина линии связи, начиная с которой атака с расщеплением числа фотонов становится эффективной, больше, чем длина, на которой определяющую роль начинают играть темновые отсчёты, которые фактически и лимитируют длину линии связи.

Результаты разработки дистанционного курса по физическим основам квантовой криптографии

Рассмотрим описание функциональных возможностей курса по физическим основам квантовой криптографии в системе управления обучением MOODLE. Непрерывное совершенствование системы высшего педагогического образования в условиях информационного общества выдвигает на передний план теории и практики новые проблемы, связанные с необходимостью переноса части образовательного процесса в информационно-образовательное пространство Интернета. Рассмотрим процесс создания дистанционного курса по физическим основам квантовой криптографии в системе управления обучением MOODLE. Курс посвящён изучению фундаментальных идей квантовой криптографии, криптографических концепций и инструментов таких, как определения безопасности, минимальная энтропия, усиление конфиденциальности, а также протоколов и доказательств безопасности для распределения квантовых ключей, основ независимой от устройства квантовой криптографии, современных квантовых криптографических задач и протоколов. Курс знакомит нас с основными понятиями, такими как квантовая криптография, квантовое шифрование и дешифрование, шифр, ключ, открытый текст, вскрытие шрифта, с классификацией криптографических алгоритмов, с основоположником современной криптографии — Клодом Шенноном, его жизнью и незаменимым вкладом в развитие данной науки (дал определение абсолютно стойкого шрифта и указал возможные методы взлома криптоалгоритма). Представим тематическое планирование элективного курса по квантовой криптографии в виде списка:

1. Квантовые технологии — обзор. Введение в квантовую теорию информации, теорема о запрете на квантовое клонирование
2. Квантовая криптография по протоколу BB84. Протокол BB84 и атаки на него
3. Некоторые другие протоколы: с шестью состояниями, B92, SARG
4. Исправление ошибок ключа
5. Энтропийные соотношения неопределённостей, доказательства стойкости и усиление секретности
6. Протокол с обманными состояниями
7. Запутанные состояния, неравенства Белла и протокол E91
8. Протоколы с непрерывными наблюдаемыми
9. Аппаратное обеспечение для квантовой криптографии
10. Проблема декогеренции. Декогеренция и её причины. Масштабы времени декогеренции
11. Методы преодоления декогеренции. Квантовая коррекция ошибок

На рис. 1 приведено изображение элементов первой темы дистанционного курса по физическим основам квантовой криптографии, созданного в системе управления обучением MOODLE.

На рис. 2 приведено изображение элементов второй темы дистанционного курса по физическим основам квантовой криптографии, созданного в системе управления обучением MOODLE.

На рис. 3 приведено изображение первой части структуры дистанционного курса по физическим основам квантовой криптографии, созданного в системе управления обучением MOODLE.

На рис. 4 приведено изображение второй части структуры дистанционного курса по физическим основам квантовой криптографии, созданного в системе управления обучением MOODLE.

Среди элективных курсов особое место может занять разработанный дистанционный курс по физическим основам квантовой криптографии. Основные задачи изучения

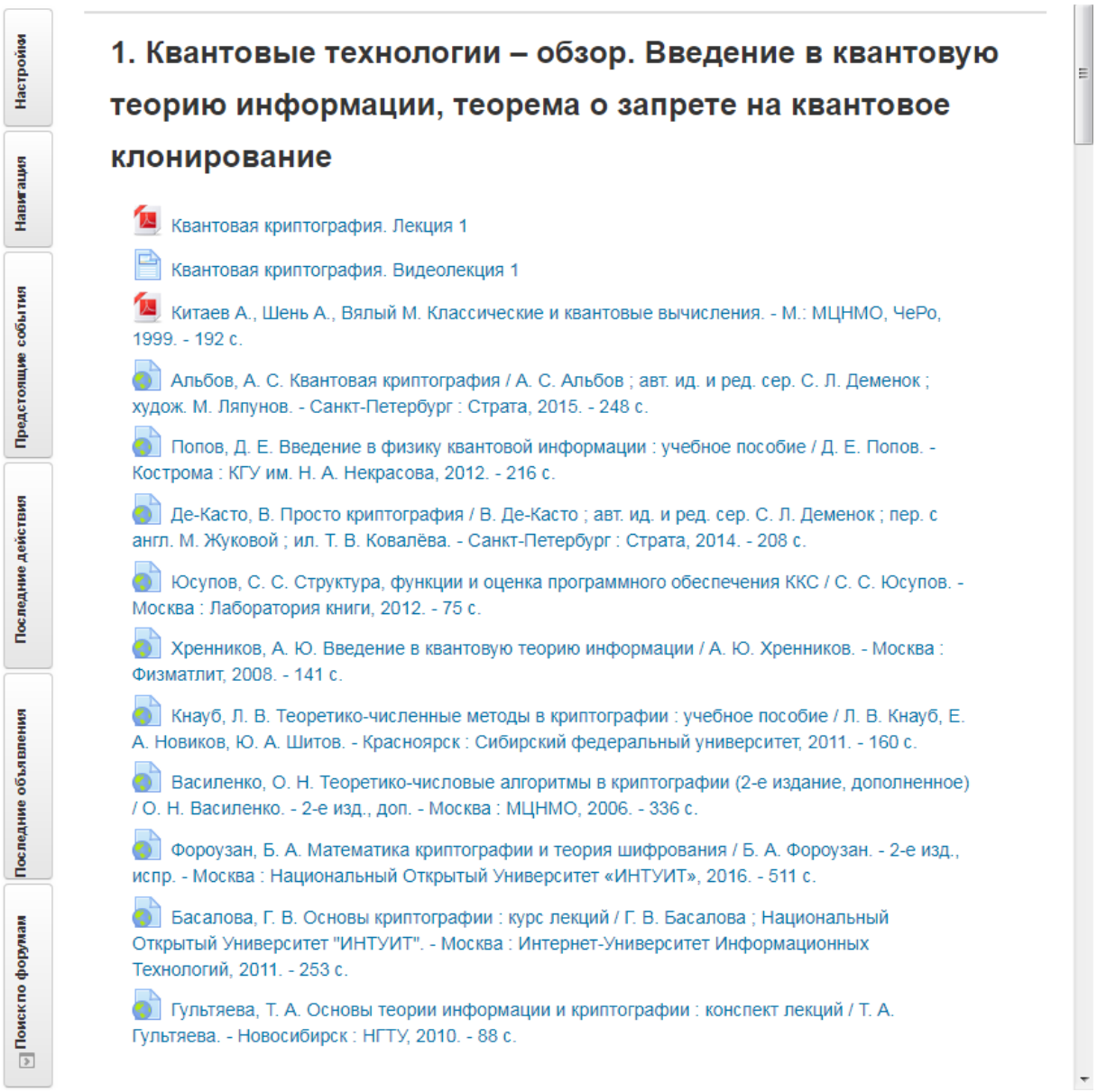

Рис. 1. Элементы первой темы дистанционного курса по физическим основам квантовой криптографии в системе дистанционного обучения на платформе MOODLE.

дистанционного курса по физическим основам квантовой криптографии состоят в развитии у студента логики мышления, интуиции и творческих способностей; овладении системой знаний и умений по криптографии для последующего обучения её в ВУЗах; применение компьютера для эффективного шифрования информации; изучение математического пакета Maple для последующего его применения в шифровании данных.

Правильная подборка задач поможет закрепить изученный материал и подготовить студента к решению задач по квантовой криптографии.

Теоретические материалы курса по физическим основам квантовой криптографии

При $L_1 < L < L_5$ (L_1, L_5 — длины, начиная с которых Ева может блокировать все посылки вплоть до пятифотонных) критическая длина линии связи в этом диапазоне определяется лишь темновыми отсчётами на приёмной стороне и энтропией фон Неймана источника квантовых состояний на передающей стороне.

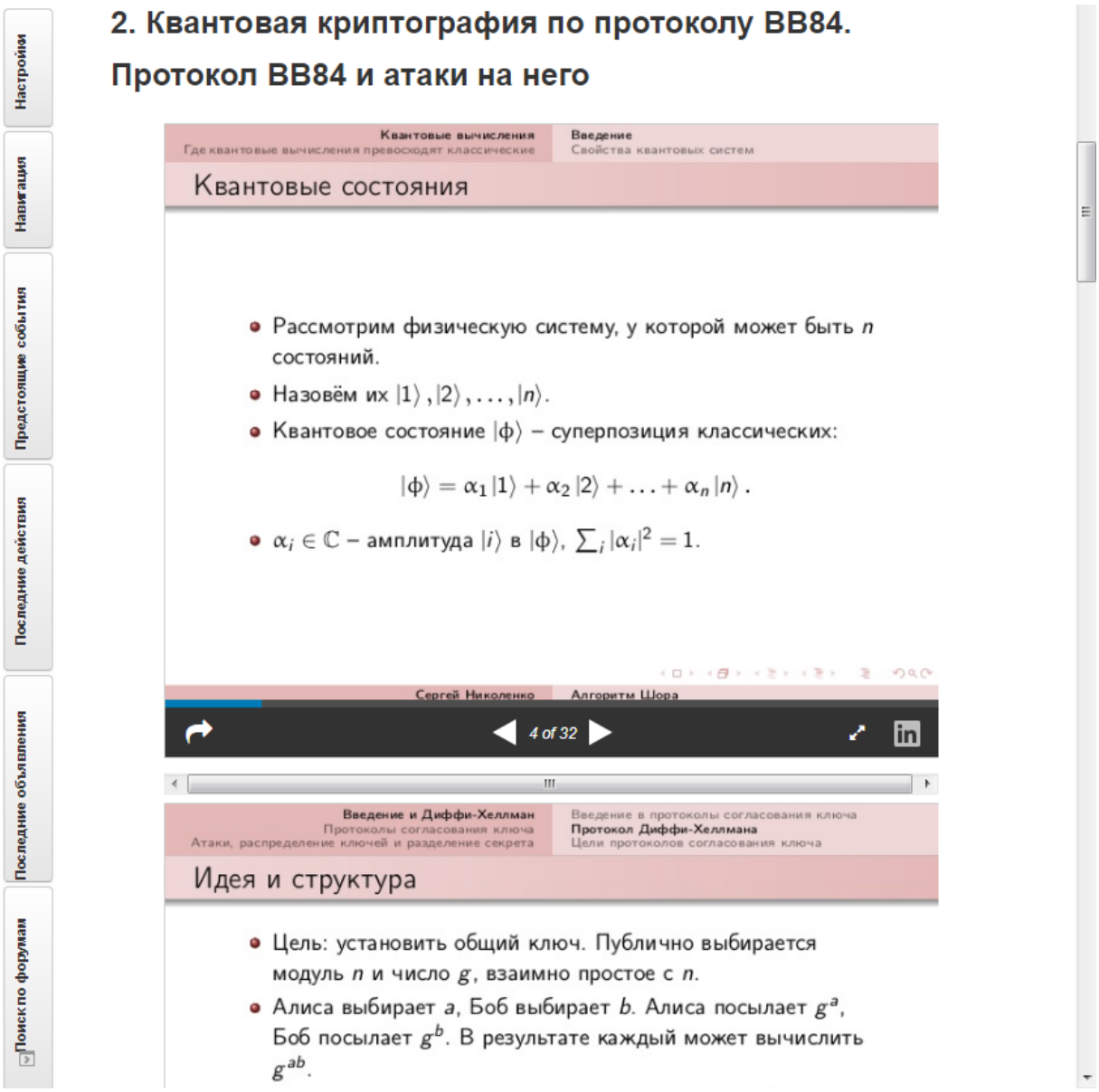

Рис. 2. Элементы второй темы дистанционного курса по физическим основам квантовой криптографии в системе дистанционного обучения на платформе MOODLE.

Однофотонные информационные состояния в квантовом протоколе связи с фазово-временным кодированием в базисах $+$, L, $\times$, L имеют вид [14]:

$$\|0,+L\rangle = \cos\left(\frac{\alpha}{2}\right)|1\rangle + \sin\left(\frac{\alpha}{2}\right)|2\rangle\ , \tag{1}$$

$$|1,+L\rangle = \cos\left(\frac{\alpha}{2}\right)|1\rangle - \sin\left(\frac{\alpha}{2}\right)|2\rangle\ . \tag{2}$$

$$|0,\times L\rangle = -\sin\left(\frac{\alpha}{2}\right)|1\rangle + \cos\left(\frac{\alpha}{2}\right)|2\rangle\ , \tag{3}$$

$$|1,\times L\rangle = \sin\left(\frac{\alpha}{2}\right)|1\rangle + \cos\left(\frac{\alpha}{2}\right)|2\rangle\ , \tag{4}$$

соответственно, в базисах и $+, R$ и x, R, имеем

$$|0,+R\rangle = \cos\left(\frac{\alpha}{2}\right)|2\rangle + \sin\left(\frac{\alpha}{2}\right)|3\rangle\ , \tag{5}$$

$$|1,+R\rangle = \cos\left(\frac{\alpha}{2}\right)|2\rangle - \sin\left(\frac{\alpha}{2}\right)|3\rangle\ . \tag{6}$$

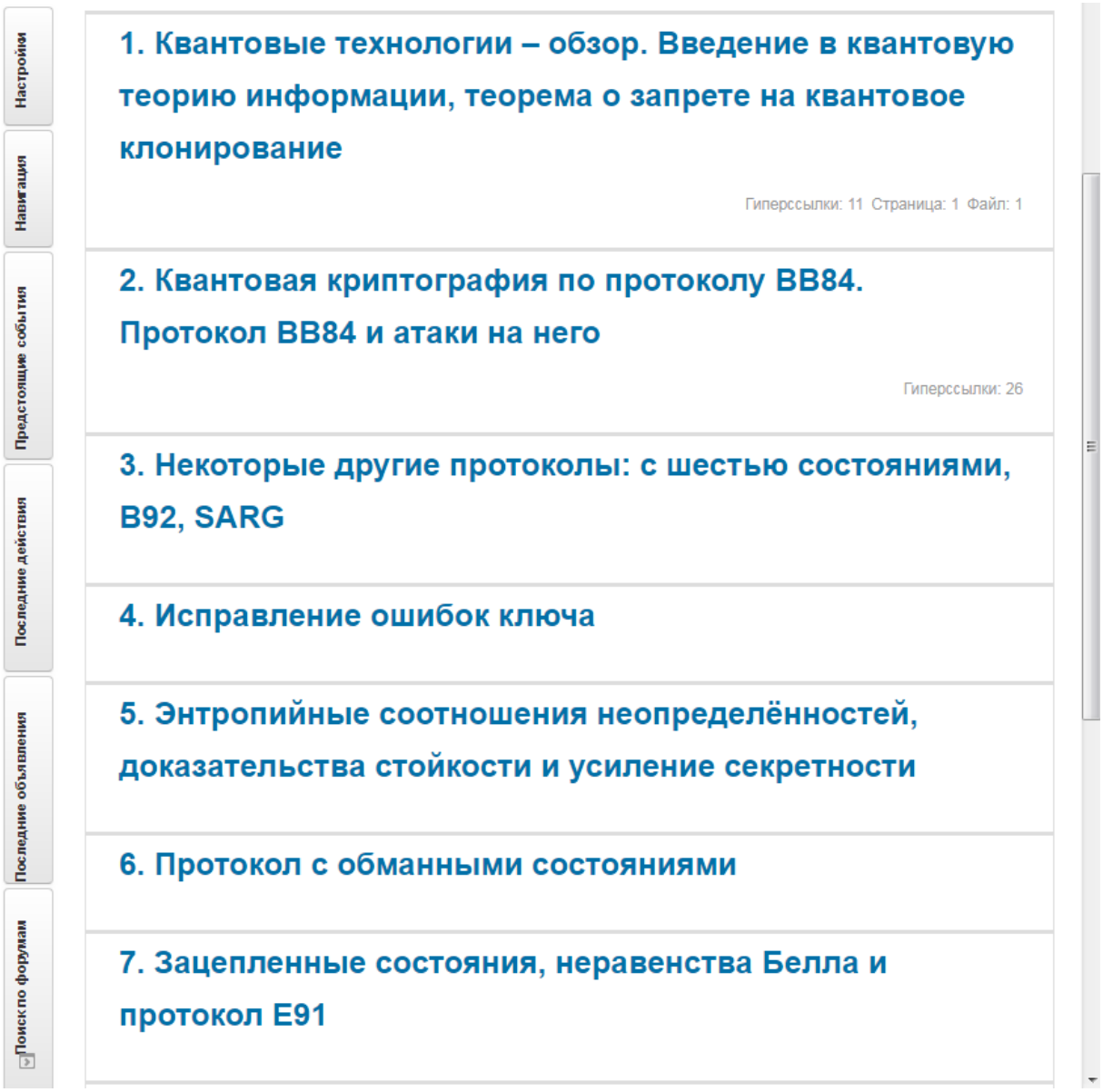

Рис. 3. Первая часть структуры дистанционного курса по физическим основам квантовой криптографии в системе дистанционного обучения на платформе MOODLE.

$$|0, \times R\rangle = -\sin\left(\frac{\alpha}{2}\right)|2\rangle + \cos\left(\frac{\alpha}{2}\right)|3\rangle\ , \tag{7}$$

$$|1, \times R\rangle = \sin\left(\frac{\alpha}{2}\right)|2\rangle + \cos\left(\frac{\alpha}{2}\right)|3\rangle\ . \tag{8}$$

Здесь $|\iota\rangle$-$\iota = 1, 2, 3$ — локализованные состояния во временных слотах 1, 2, 3, которые сдвинуты по времени на одинаковую величину.

Выберем состояния внутри базисов L и R неортогональными $\langle 0 + L|1 + L\rangle = {}^{-}\langle O \times L|1 \times L\rangle = \cos(\alpha)$, как в протоколе $B92$, а между базисами $+L$ и $\times L(+R$ и $\times R)$ частично ортогональны $\langle 0 + L|0 \times L\rangle = \langle 1 + L|1 \times L\rangle = 0(\langle 0 + R|0 \times R\rangle = \langle 1 + R|1 \times R\rangle = 0)$. Аналогично и в базисе R. Информационные неоднофотонные состояния получаются ослаблением когерентного состояния. Поскольку от посылки к посылке относительная фаза в состояниях не фиксирована, то подслушиватель видит в канале связи усреднён-

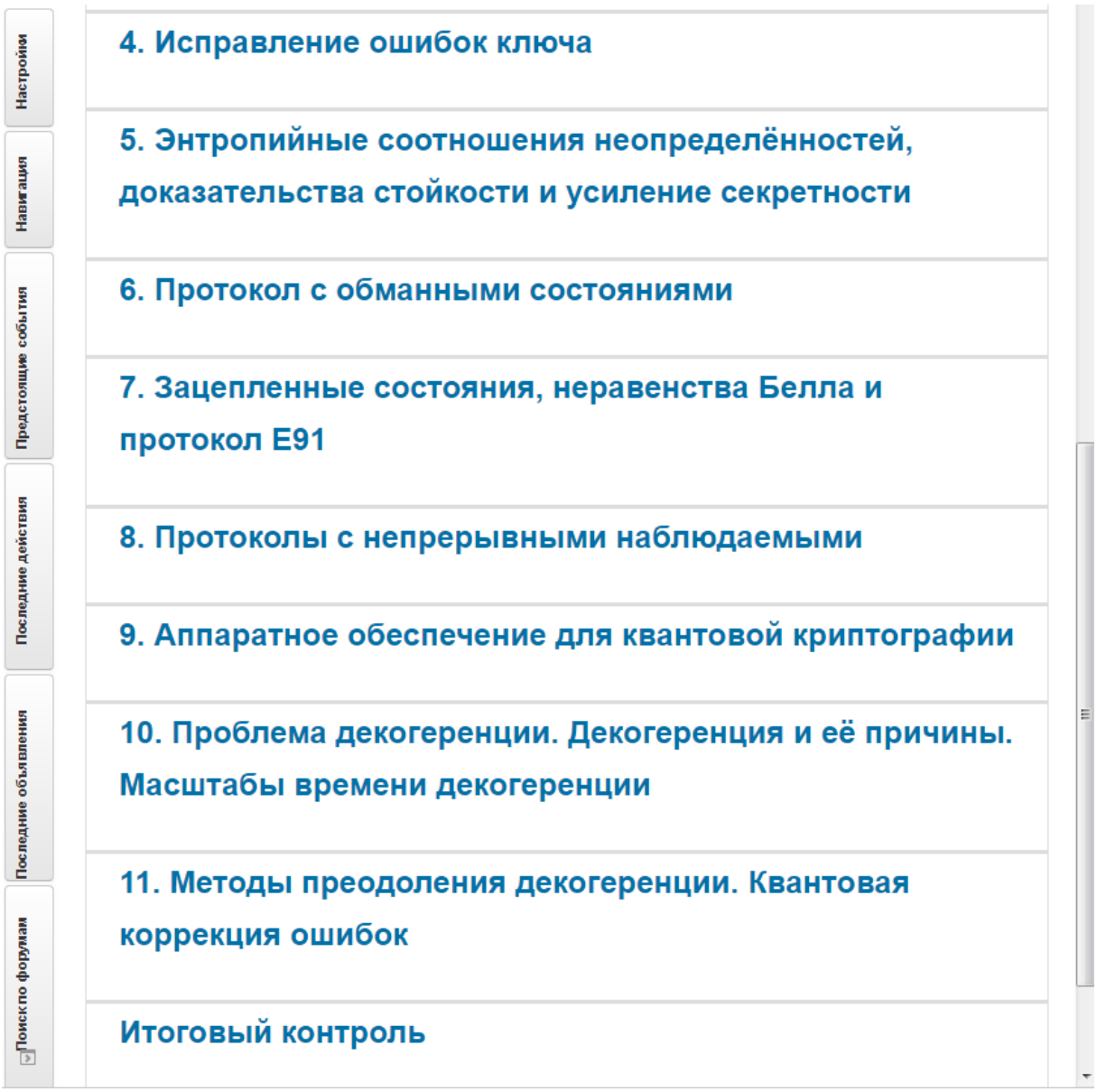

Рис. 4. Вторая часть структуры дистанционного курса по физическим основам квантовой криптографии в системе дистанционного обучения на платформе MOODLE.

ное по фазе когерентное состояние

$$\begin{aligned} \rho_A(i,b) = \oplus_{k=0}^{\infty} p_k (|i,b\rangle^{\otimes k})(^{\otimes k}\langle i,b|) \ , \\ p_k = \frac{\mu^k}{k!} \ , \\ i = 0,1, \ \ b = +L, \times L, +R, \times R \ , \end{aligned} \tag{9}$$

где μ – среднее число фотонов в когерентном состоянии. Рассмотрение ниже годится и для источника с произвольным распределением по числу фотонов, а не только когерентного состояния.

Проведём анализ измерений на приёмной стороне. Перейдём теперь к измерениям на приёмной стороне. Боб случайно и равновероятно выбирает измерения в одном из двух

базисов. Формально измерения описываются следующими разложениями единицы:

$$I = A_{0,b} + A_{1,b} + A_{x,b},\ A_{0,b} = \frac{I - 1|1,b\rangle\langle 1,b|}{1 + |\langle 0,b|1,b\rangle|}\ , \tag{10}$$

$$A_{1,b} = \frac{I - 1|0,b\rangle\langle 0,b|}{1 + |\langle 0,b|1,b\rangle|},\ A_{x,b} = I - A_{0,b} - A_{1,b}\ . \tag{11}$$

Измерения аналогичны измерениям в протоколе B92 Измерения (10) обладают тем свойством, что ненулевой результат в канале $A_{0,b}$ возникает только от состояния $|0,b\rangle$, и никогда от состояния $|1,b\rangle$. Аналогично для исходов в канале $A_{1,b}$. Отсчёты в канале $A_{1,b}$ отвечают результатам с неопределённым исходом, такие отсчёты отбрасываются. Вероятность отсчётов с определённым исходом есть

$$Pr\{|0,b\rangle\langle 0,b|A_{0,b}\} = Pr\{|1,b\rangle\langle 1,b|A_{1,b}\} = 1 - \cos(\eta)\ . \tag{12}$$

После отбрасывания результатов с неопределённым исходом информация Боба в битах в пересчёте на одну оставленную позицию составляет $I\left(A;B\right) = 1$ (при идеальных фотодетекторах). Учтём теперь неидеальность фотодетекторов.

С учётом потерь вероятность достижения информационными состояниями приёмной стороны есть

$$P_{detected} = \left(1 - e^{-\mu} - (e^{-\mu\Gamma} - e^{-\mu})(1 - \cos\left(\alpha\right)\right)\ . \tag{13}$$

Данная величина равна доле непустых посылок. Все лавинные фотодетекторы в телекомуникационном диапазоне длин волн $1.3 - 1.55$ мкм работают в стробируемом режиме. Фотодетектор активируется посредством подачи короткого импульса напряжения длительности 1-2 не в момент возможного прихода информационного состояния. Темновые отсчёты с определённой вероятностью имеют место в момент стробирования независимо от прихода состояния.

Рассмотрим квантовые эффективности фотодетекторов и вероятности фотоотсчётов. Пусть квантовые эффективности фотодетекторов равны η_0 и η_1 учётом (13) вероятность детектирования информационных состояний 0 и 1 в окне стробирования равна $\eta_{0,1}(L) = \frac{1}{2}P_{detected}\eta_{0,1}$. Темновые отсчёты возникают только в моменты стробирования, вероятность темнового отсчёта во временном окне строба есть $p_{d0}^{(0)}$ и $p_{dark}^{(1)}$. Фотоотчёты в детекторах $\bar{D_0}$ и $\bar{D_1}$ можно разбить на следующие множества (рис. 5). A_0 и A_1 – множества отсчётов от информационных состояний. D_0 и D_1 – множества темновых отсчетов соответственно в детекторе $\bar{D_0}$ и $\bar{D_1}$ Напомним, что оба детектора стробируются одновременно, поэтому темновые отсчёты могут иметь место одновременно (в одном и том же стробе) в двух фотодетекторах.

A_1 – множество одновременных отсчётов только от информационных состояний A_0 и темновых отсчётов D_0 (аналогично для множества A_7). A_2 – множество одновременных отсчётов только от информационных состояний A_0 и темновых отсчётов в детекторе D_1 (аналогично для A_5). A_3 – множество одновременных отсчётов от A_0, D_0 и D_1. Аналогично для множества отсчётов A_6. A_4 – множество одновременных отсчётов только от D_0 и D_1. Множества A_0 и A_1 не пересекаются, поскольку Алиса посылает либо 0, либо 1. Одновременные события в одном временном стробе в одном детекторе от информационного состояния и темнового шума воспринимаются как один фотоотсчёт. Одновременные фотоотсчёты в двух детекторах в одном временном стробе отбрасываются. Вероятность отсчёта от информационных состояний 0 и 1 равна

$$\begin{aligned} Pr\{info\} &= Pr\{A_0 + A_1 - A_0 \cap D_1 - A_1 \cap D_0\} = \\ &= \eta_0\left(L\right) + \eta_1\left(L\right) - \eta_0\left(L\right)p_{dark}^{(0)} - \eta_1\left(L\right)p_{dark}^{(1)}\ . \end{aligned} \tag{14}$$

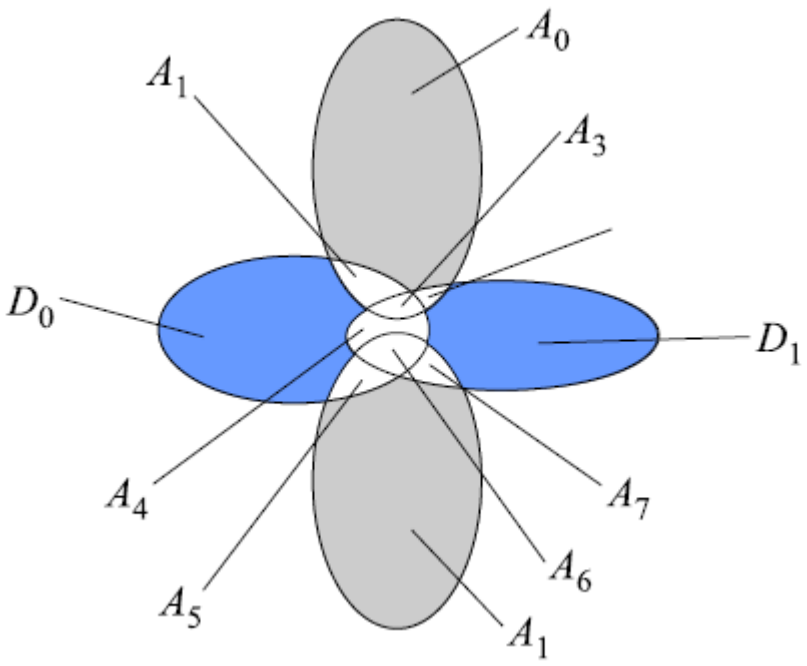

Рис. 5. Различные множества событий фотоотсчётов.

Вероятность исходов только от темновых отсчётов равна (напомним, что одновременные отсчёты в двух детекторах отбрасываются)

$$\begin{aligned} Pr\{dark\} = \\ = Pr\{D_0 + D_1 - 2(D_0 \cap D_1 - \\ -A_0 \cap D_0 \cap D_1 - A_1 \cap D_0 \cap D_1) - \\ -(A_0 \cap D_0 - A_0 \cap D_0 \cap D_1) - (A_1 \cap D_0 - A_1 \cap D_0 \cap D_1) - \\ -(A_1 \cap D_1 - A_1 \cap D_0 \cap D_1) - (A_0 \cap D_1 - A_0 \cap D_0 \cap D_1)\} = \\ = p_{dark}^{(0)} + p_{dark}^{(1)} - (\eta_0(L) + \eta_1(L))(p_{dark}^{(0)} + p_{dark}^{(1)}) + \\ +4(\eta_0(L) + \eta_1(L)\, p_{dark}^{(0)} p_{dark}^{(1)} - 2p_{dark}^{(0)} p_{dark}^{(1)} . \end{aligned} \tag{15}$$

Поскольку состояния, отвечающие 0 и 1, посылаются равновероятно, то только половина из каждого непересекающегося множества темновых отсчётов будет давать правильные отсчёты. Другая половина отсчётов будет ошибочной. Для вероятности ошибки на приёмной стороне у Боба имеем

$$Q(L) = \frac{\frac{1}{2} Pr\{dark\}}{Pr\{info\} + Pr\{dark\}} . \tag{16}$$

Ошибка принимает особенно простое выражение при $\eta_0(L) = \eta_1(L) = \eta(L)$, $p_{dark}^{(0)} = p_{dark}^{(1)} = p_{dark}$. С точностью до линейных членов по $\eta(L)$, p_{dark}, имеем

$$Q(L) = \frac{\frac{1}{2} P_{dark}}{\eta(L) + p_{dark}} . \tag{17}$$

Взаимная информация между Алисой и Бобом после исправления ошибок случайными кодами не превышает пропускной способности классического симметричного бинарного канала связи с величиной ошибки $Q(L)$. Имеем

$$I(A;B) \leq C_{class}(Q) = 1 - H(Q(L)) , \tag{18}$$

$$H(x) = -x \log x - (1-x) \log(1-x) . \tag{19}$$

Проведём анализ действий подслушивателя. Рассмотрим теперь действия подслушивателя. Поскольку фотодетекторы на приемной стороне не различают число фотонов, то Боб может следить лишь за сохранением общего числа посылок на приёмной стороне при известной длине линии связи. Вероятность потерь или доля посылок, исчезающих в канале связи длины L — есть

$$p_{loss}(L) = \sum_{k=1}^{\infty} p_k (1 - \Gamma(L))^k \,, \tag{20}$$

$$\Gamma(L) = 10^{-\frac{\alpha L}{10}} \,. \tag{21}$$

здесь $\alpha \approx 0.2$ дБ/км – константа затухания в одномодовом оптоволокне. Для когерентного состояния доля потерянных посылок составляет $p_{loss}(L) = \epsilon^{-\mu\Gamma} - \epsilon^{-\mu}$ (при $L \to \infty$, $\Gamma(L) \to 0$, $p_{loss}(L) \to 1 - \epsilon^{-\mu}$ – исходная общая доля непустых посылок). Будем рассматривать ситуацию при больших длинах ($L > L_1$ ($p_{loss}(L_1) = p_1$), когда Ева может блокировать все однофотонные посылки, при атаке на которые она неизбежно производила бы ошибки на приёмной стороне. С дальнейшим ростом длины линии подслушиватель может блокировать двух, трёх, k-фотонные посылки. Иначе говоря, при длинах $L < L_1 < L < L_2 < L... < L_k...$ Ева может блокировать частично, а начиная с некоторой длины, полностью k-фотонные посылки. Зависимости длин L_k от среднего числа фотонов μ в когерентном состоянии приведены на рис. 6.

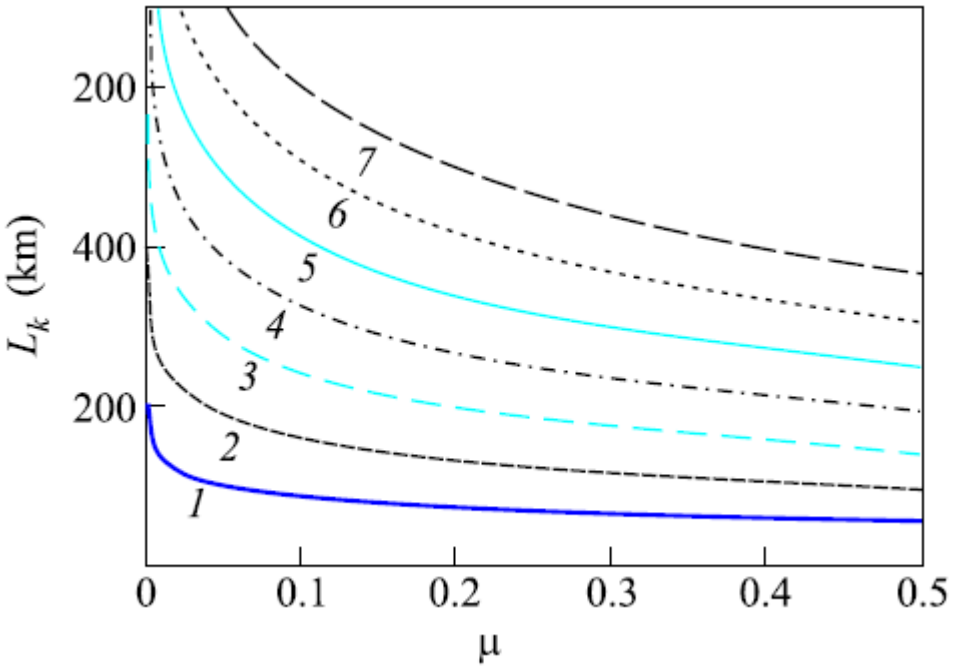

Рис. 6. Зависимость длины линии L_k от среднего числа фотонов μ в когерентном состоянии, начиная с которых Ева может блокировать посылки, содержащие k фотонов.

Доля оставшихся посылок при длине L, которые Ева не может блокировать и вынуждена сохранить, составляет

$$p_k(L) = p_k\left(1 - \theta\left(p_{loss}(k, L)\right)\right) + \\ + \left(p_k - p_{loss}(k, L)\right)\theta\left(p_{loss}(k, L)\right)\theta\left(p_k - p_{loss}(k, L)\right) \,. \tag{22}$$

Далее из каждой посылки, содержащей $k > 1$ фотонов, Ева один фотон направляет к Бобу через свой канал связи с меньшими потерями (в предельном случае вообще без

потерь), а остальные оставляет у себя в квантовой памяти до процедуры разглашения базисов легитимными пользователями. Однако даже после разглашения базисов из-за неортогональности состояний внутри базиса Ева не будет достоверно знать каждый передаваемый бит.

Проведём расчёт квантовой пропускательной способности квантового канала связи. При длине линии связи $L > L_1$, после разглашения базисов, Ева имеет в каждой ячейке квантовой памяти состояние

$$\begin{aligned} p_E(0,b) &= p \oplus_{k=2}^{\infty} p_k(L)(|0,b\rangle^{\oplus(k-1)})({}^{\oplus(k-1)}\langle 0,b|) \ , \\ p_E(1,b) &= p \oplus_{k=2}^{\infty} p_k(L)(|1,b\rangle^{\oplus(k-1)})({}^{\oplus(k-1)}\langle 1,b|) \ . \end{aligned} \tag{23}$$

здесь базис b считается известным.

Количество информации в битах на одну посылку $I\,(;\,)$, которое может быть получено из ансамбля квантовых состояний (23), ограничено сверху фундаментальной границей Холево, которая является достижимой и совпадает с классической пропускной способностью $\bar{C}(L)$ квантового канала связи между Алисой и Евой с информационными состояниями (24) [14]. Имеем

$$I(A;E) \leq \bar{C}(L) = \sum_{m=2}^{\infty} \bar{p}_m(L)\bar{C}(\cos^{m-1}(\alpha)) \ . \tag{24}$$

Здесь

$$\begin{aligned} \bar{p}_m(L) = (L)/N(L), N(L) &= \sum_{m=2}^{\infty} p_m(L) \ , \\ \bar{C}(x) &= \left(-\frac{1-x}{2}\right)\log\left(\frac{1-x}{2}\right) - \\ &- \left(\frac{1+x}{2}\right)\log\left(\frac{1+x}{2}\right) \end{aligned} \tag{25}$$

классическая пропускная способность квантового канала связи [14]. Из (24), (25) следует, что информация Евы о передаваемом ключе фактически определяется энтропией фон Неймана источника на передающей стороне Алисы, в котором распределение по числам заполнения фотонов сдвинуто на единицу, поскольку один фотон должен быть направлен на приёмную сторону к Бобу.

Распространение ключей возможно [14], если $I\,(;\,) < I\,(;\,)$. Критическая длина линии определяется как корень уравнения $I\,(;\,) = I\,(;\,)$, имеем

$$C_{class}(Q) = \bar{C}(L) \ , \tag{26}$$

$$1 - H(Q(L)) = \sum_{m=2}^{\infty} \bar{p}_m(L)\bar{C}\left(\cos^{m-1}(\alpha)\right) \ . \tag{27}$$

Зависимости взаимных информации $I\,(A;E)$ и $I\,(A;B)$ от длины оптоволоконной линии связи при различной вероятности темновых отсчётов представлены на 7. Критическая длина линии связи, до которой возможно распределение ключей, определяется точкой, где разность $I\,(A;B) - I\,(A;E)$ обращается в нуль. Фактически разность $I\,(A;B) - I\,(A;E)$ представляет собой количество информации в битах, которое является ключом.

Как следует из рис. 5, при вероятности темновых отсчетов $p_{dark} = 10^{-5}$ отсч/строб, предельная длина линии связи составляет $\approx$ 80 км. Такой уровень темновых отсчётов является типичным при охлаждении лавинных фотодетекторов до температуры

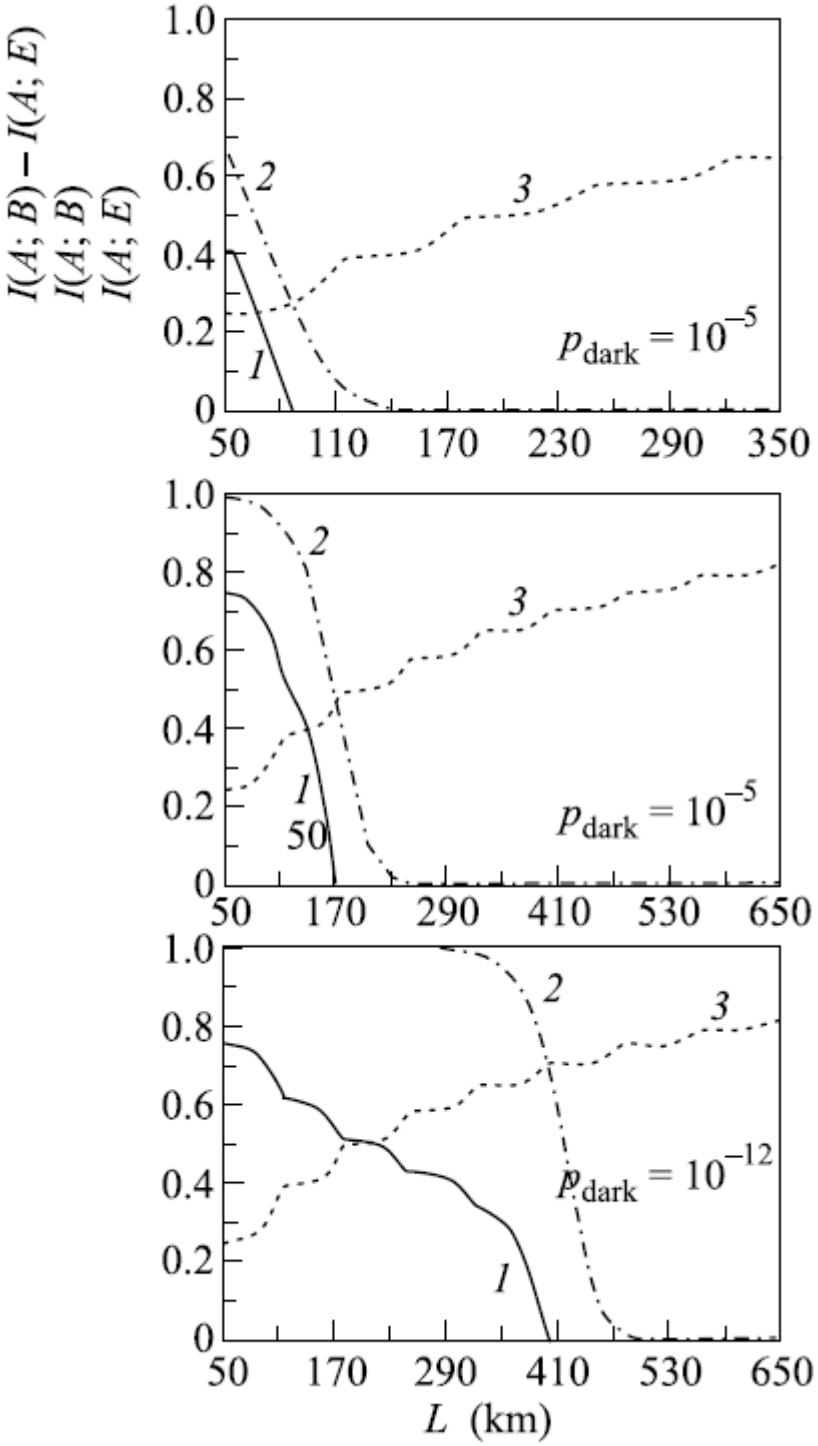

Рис. 7. Кривые 1 отвечают зависимости $I(A;B) - I(A;E)$ от длины линии связи L, кривые 2 — зависимостям $I(A;B)$ и 3 — зависимостям $I(A;E)$. Вероятности темновых отсчётов приведены непосредственно на рисунке. Квантовая эффективность фотодетекторов и среднее число фотонов в когерентном состоянии одинаковы для всех кривых и равны соответственно $\eta = 0.1$, $\mu = 0.2$. Угол между состояниями $\alpha = \pi/8$.

$\approx -50-60$. При охлаждении до азотных температур достижим уровень темновых шумов $p_{dark}=10^{-7}$ отсч/строб. Предельная длина линии связи в этом случае составляет ≈ 170 км. И, наконец, при вероятности темновых отсчётов $p_{dark}=10^{-12}$ отсч/строб достижима длина в 400 км. Такой уровень темновых отсчётов достигается в ряде экспериментов для сверхпроводящих детекторов на основе NbN.

Сделаем замечание по стратегии передачи вероятностной информации. Описанная выше стратегия даёт Еве вероятностную информацию о битах ключа [14]. Ева может в принципе использовать стратегию, которая даёт ей достоверную информацию о каждом передаваемом бите. Поскольку имеется 4 базиса, $+L$, $\times L$ и $+R$, $\times R$, и внутри базисов состояния неортогональны, то для того, чтобы получить достоверную информацию, Еве необходима как минимум пятифотонная компонента. Ева использует 4 фотона для измерений, которые аналогичны (10). Пятый фотон направляется к Бобу только в том случае, если получен результат с определенным исходом для измерений над всеми четырьмя фотонами (исходы $A_{0,1,+L}$, $A_{0,1,\times L}$ и $A_{0,1,+R}$, $A_{0,1,\times R}$). Это даёт возможность Еве после раскрытия базисов однозначно определить передаваемый бит. Если получен результат измерения с неопределённым исходом ${}_{0,b}$, хотя бы для одного из четырёх фотонов, то посылка блокируется. Вероятность исхода с определенным результатом для четырёх фотонов $-\left(1^{-}\cos\left(\alpha\right)\right)^{4}$ (например, при $\alpha=\pi/8$ эта величина меньше 10^{-4}). Это означает, что Ева должна будет блокировать почти все пятифотонные посылки (долю посылок $>1-10^{-4}$).

Такая стратегия возможна, если длина линии связи превышает $L>L_5$. Однако, как следует из рис. 6 и рис. 7 при типичных рабочих значениях среднего числа фотонов в состоянии $\mu=0.1-0.2$, взаимная информация $I\left(A;E\right)$ сравнивается со взаимной информацией $I(A;B)$ при меньших длинах, чем L_5, поэтому данная атака Евы неэффективна. Уже при меньших длинах определяющую роль начинают играть темновые отсчёты, которые, по существу, определяют критическую длину.

Рассмотрим расщепление числа фотонов. Любая экспериментальная реализация с использованием фотонов протокола распределения квантового ключа с двумерными квантовыми состояниями должна идеально выполняться с однофотонным источником. К сожалению, это очень сильное требование с современными технологиями, и нужно проектировать способ экспериментального аппроксимации однофотонного источника. Несмотря на то, что распределение квантовых ключей оказалось безоговорочно безопасным, это может быть не так, если технология честных сторон не идеальна.

В большинстве существующих реализаций однофотонный импульс аппроксимируется слабым когерентным импульсом $\left|\mu e^{i\theta}\right\rangle$. Как сказано выше, и поскольку нет абсолютной опорной фазы, состояние, наблюдаемое Бобом и Евой, представляет собой некогерентную смесь многофотонных состояний с пуассоновскими вероятностями. Затем Ева может выполнить измерение числа фотонов без сноса, сохранить один из фотонов, когда найдено многофотонное состояние, и передать остальным Бобу. Обратите внимание, что действие Евы не обнаружено Бобом, если предполагается, что он имеет доступ только к средней скорости обнаружения, а не к статистике фотонов, которые он получает. Предполагаем, что Еве способно контролировать потери на линии, соединяющей Алису и Боба (или, что эквивалентно, она может отправлять фотоны Бобу по линии без потерь). В этой ситуации Ева может выполнить так называемую атаку на расщепление числа фотонов, которая, как показано ниже, ограничивает безопасность многих известных существующих протоколов.

Рассмотрим протокол BB84. В протоколе BB84 [15] Алиса выбирает случайным образом между двумя взаимно несмещенными основаниями, в которых она кодирует классический бит. Обозначая $|\pm x\rangle$ ($|\pm y\rangle$) собственные векторы σ_x (σ_y) с собственным значением ±1, она может закодировать логический 0 в либо $|+x\rangle$, либо $|+y\rangle$, а 1 в $|-x\rangle$ или

$|-y\rangle$. Она отправляет кубит Бобу, который измеряет случайным образом в x или y основе. Затем они сравнивают базис, и когда они совпадают, бит принимается. Таким образом, половина символов отбрасывается и, в отсутствие возмущений, они заканчиваются общим секретным ключом. В практических ситуациях, а также из-за наличия ошибок и, возможно, шпиона, необходимо применять некоторые методы коррекции ошибок и усиления конфиденциальности, чтобы извлечь более короткий полностью безопасный ключ.

Теперь давайте посмотрим, как Ева может воспользоваться многофотонными импульсами. Алиса посылает импульс с $\mu \ll 1$, кодирующим классический бит (скажем, при поляризации света). Ева выполняет измерение количества фотонов, а когда обнаруживаются два или более фотонов, она берет один и передает остальным Бобу по своей линии без потерь. Ева хранит фотон в квантовой памяти и ждёт до примирения базиса. Как только база объявлена, ей нужно только различать два ортогональных состояния, которые можно детерминировать. Таким образом, для всех многофотонных импульсов Ева получает всю информацию о посланном бите. Если Алиса и Боб в принципе связаны линией с потерями, Ева может блокировать некоторые импульсы одиночных фотонов и направить многофотонные импульсы, на которых она может получить всю информацию, своей линией без потерь. Таким образом, Алиса и Боб не замечают никаких изменений в ожидаемой исходной скорости, и Ева остается незамеченной. Когда потери таковы, что Ева может блокировать все однофотонные импульсы, протокол перестает быть безопасным.

Обозначим через α потери в дБ за км на линии. Ожидаемая скорость передачи со стороны Боба даётся по уравнению

$$R_{Bob} = \mu\, 10^{-\delta/10}\ [\text{photons/pulse}]\ , \tag{28}$$

где $\delta = \alpha d$ – полное затухание в дБ квантового канала длины d. Ева применит атаку расщепления числа фотонов на долю $1-q$ импульсов. Поскольку она не хочет быть обнаруженной, сырая ставка не должна изменяться, то есть она должна выбрать q таким образом, чтобы

$$R_{Bob}^{PNS} = q\mu + (1-q)\, R_{BB84} = R_{Bob}\ , \tag{29}$$

где $R_{BB84} \equiv \sum_{n=2}^{\infty} p_n(n-1)$. Информация Евы равна нулю, когда она ничего не делает, и одна для атаки на расщепление числа фотонов, то есть, обозначая $S_{BB84} \equiv \sum_{n=2} p_n$,

$$I_{Eve}(q) = \frac{(1-q)\, S_{BB84}}{q + (1-q)\, S_{BB84}}\ . \tag{30}$$

Если потери таковы, что q может быть равно нулю в уравнении (29) (все однофотонные импульсы могут быть заблокированы), Ева получает всю информацию, не будучи обнаруженной. Критическое затухание, δ_c, затем задается условием $R_{BB84} = R_{Bob}$. На рис. 8 показана зависимость I_{Eve} от d для $\mu = 0.1$ и $\alpha = 0.25\text{dB/km}$. Критическое затухание в этом случае равно $\delta_c = 13\,\text{dB}$, а соответствующее расстояние $d_c = 52\,\text{км}$. Здесь необходимо подчеркнуть два важных момента. Во-первых, не претендуем на оптимальность стратегий расщепления числа фотонов, которые рассматриваем в этом разделе, с точки зрения информации Евы о потерях ниже δ_c. Действительно, когда потери начинают иметь значение, Еве удобнее выполнять атаку расщепления числа фотонов на все многофотонные импульсы и блокировать некоторые из однофотонных импульсов. Можно видеть, что это немного увеличивает I_{Eve}, но не изменяет критическое расстояние. Во-вторых, можно предложить альтернативные и более консервативные определения критического расстояния. Для простоты не рассматриваем возмущений в отсутствие

Евы, то есть информация Алиса-Боб, I_{AB}, является единичной. Но в реальных ситуациях и из-за наличия ошибок (например, из-за детектора и оптического шума) это неверно, и критическое расстояние соответствует точке, где $I_{Eve} = I_{AB}$. Если частота ошибок важна, это расстояние может быть меньше указанного здесь. В любом случае, для ослабления канала, превышающего δ_c, реализация протокола BB84 с использованием слабых когерентных импульсов небезопасна.

Можно задаться вопросом, возможна ли эта атака только потому, что информация закодирована при поляризации света. Однако те же рассуждения действительны и для других кодировок, таких как, например, в схеме временного бункера. Там информация передается с использованием относительной фазы между двумя слабыми когерентными импульсами, которые посылаются через волокно. В принципе, состояние, покидающее сторону Алисы,

$$|\phi\rangle = \left|\mu e^{i\theta}\right\rangle \left|\mu e^{i\theta} e^{i\phi}\right\rangle \ , \tag{31}$$

где $\phi = 0,\ \pi$ ($\phi = \pm\pi/2$) соответствуют $\pm x$ ($\pm y$). Но поскольку фазовая ссылка отсутствует, эффективное состояние, наблюдаемое Евой и Бобом,

$$\rho = \int \frac{d\theta}{2\pi} |\phi\rangle \langle\phi| = \sum_n p(n, 2\mu) |\varphi_n(\phi)\rangle \langle\varphi_n(\phi)| \ , \tag{32}$$

где $p(n, 2\mu)$ – вероятности Пуассона среднего числа фотонов 2μ и

$$|\varphi_n(\phi)\rangle = \sum_{m=0}^{n} \sqrt{\binom{n}{m} \frac{1}{2^n}}\, e^{im\phi} |n-m\rangle |m\rangle \ . \tag{33}$$

Можно определить оператор рождения и уничтожения

$$\begin{aligned} a^\dagger(\phi) &= \frac{a_1^\dagger + e^{i\phi} a_2^\dagger}{\sqrt{2}} \ , \\ a(\phi) &= \frac{a_1 + e^{-i\phi} a_2}{\sqrt{2}} \ , \end{aligned} \tag{34}$$

так что действие на двухмодовое вакуумное состояние даёт $a^\dagger(\phi)\,|0,0\rangle = |\varphi_1(\phi)\rangle$. Нетрудно видеть, что

$$|\varphi_n(\phi)\rangle = \frac{(a^\dagger(\phi))^n}{\sqrt{n!}} |0,0\rangle \ , \tag{35}$$

$[a^\dagger, a] = 1$ и $\langle\varphi_{n'}(\phi)|\,\varphi_n(\phi)\rangle = \delta_{n,n'}$. Состояние Боба задаётся выражением типа, умножающим среднее число фотонов на затухание канала. Таким образом, ситуация такая же, как и в предыдущей схеме кодирования поляризации. Ева может подсчитать общее количество фотонов в двух (ныне временных) режимах, аналогично тому, как это было в предыдущем измерении числа фотонов для поляризации, не заметив Боба. Когда обнаруживается «более одного» фотона, то есть она проектируется в $|\varphi_2\rangle$, она сохраняет одну копию состояния в её квантовой памяти до согласования базиса. Очевидно, что уравнения и критические значения в этом случае Аналогичны найденным выше для схемы кодирования поляризации.

Рассмотрим протокол B92. Альтернативная схема распределения квантового ключа задается протоколом B92. Классический бит просто кодируется Алисой с использованием двух неортогональных состояний $|\psi_0\rangle$ и $|\psi_1\rangle$ с $\langle\psi_0|\,\psi_1\rangle \neq 0$. Не теряя общности, будет принимать

$$|\psi_0\rangle = \begin{pmatrix} \cos\frac{\eta}{2} \\ \sin\frac{\eta}{2} \end{pmatrix} \qquad |\psi_1\rangle = \begin{pmatrix} \cos\frac{\eta}{2} \\ -\sin\frac{\eta}{2} \end{pmatrix} \ , \tag{36}$$

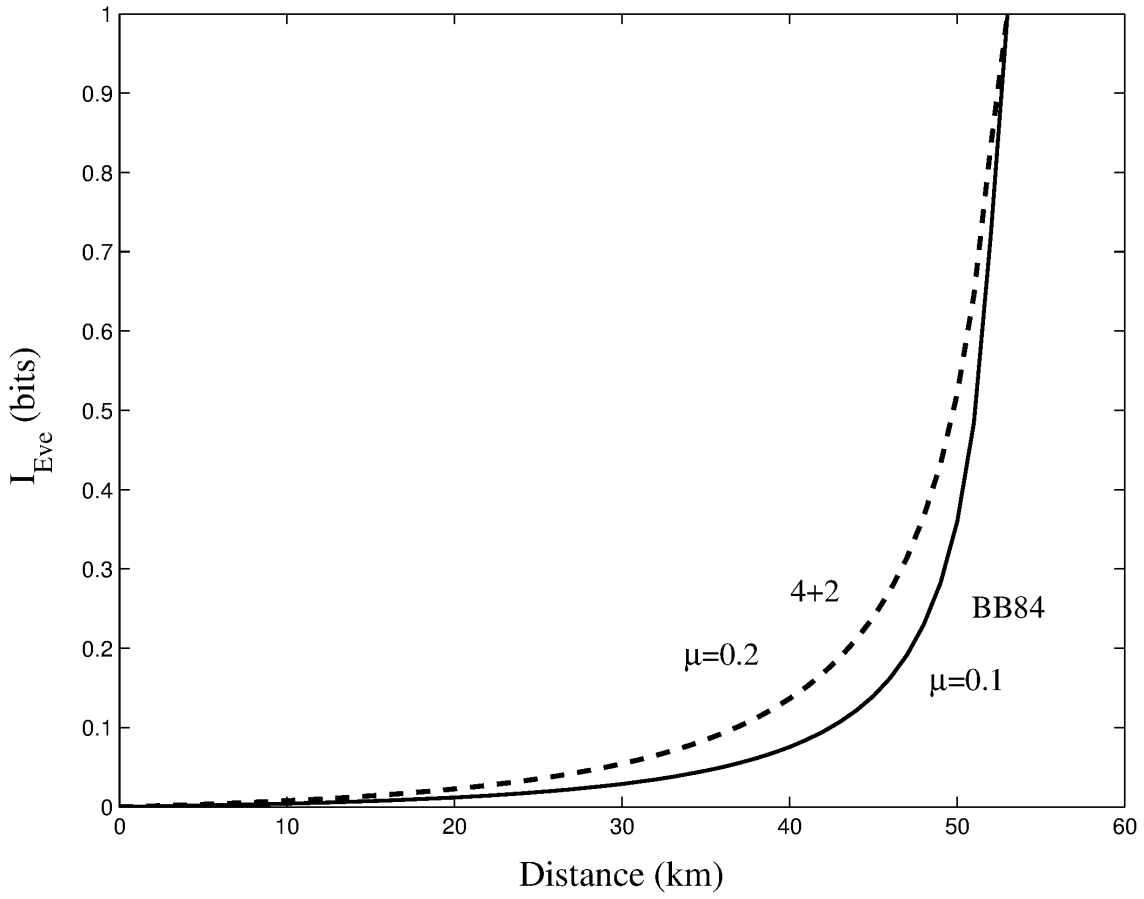

Рис. 8. Информация Евы как функция расстояния для атак с разбиением числа фотонов, описанных в тексте.

с $0 \leq \eta \leq \pi/2$ и перекрытие является $|\langle\psi_0|\psi_1\rangle| = \cos\eta$. Боб должен различать два неортогональных квантовых состояния, и это можно сделать только с некоторой вероятностью. Оптимизация измерения этой вероятности определяется следующими положительными операторами, суммирующими до одного,

$$\begin{aligned} \Pi_0 &= \frac{1}{1+\cos\eta}\left|\psi_1^{\perp}\right\rangle\left\langle\psi_1^{\perp}\right| \\ \Pi_1 &= \frac{1}{1+\cos\eta}\left|\psi_0^{\perp}\right\rangle\left\langle\psi_0^{\perp}\right| \\ \Pi_2 &= -\Pi_0 - \Pi_1 \,, \end{aligned} \tag{37}$$

где $\left|\psi^{\perp}\right\rangle$ обозначает состояние, ортогональное $|\psi\rangle$. Когда результатом измерения Боба является тот, который связан с Π_i, с $i = 0, 1$, он знает, что состояние было $|\psi_i\rangle$. Вероятность получить неубедительный результат равный перекрытию между состояниями, $p_2 = \langle\psi_0|\,\Pi_2\,|\psi_0\rangle = \langle\psi_1|\,\Pi_1\,|\psi_1\rangle = \cos\eta$. Таким образом, Алиса и Боб будут принимать отправленный бит только для тех случаев, когда измерение Боба даёт окончательный результат. Вероятность принятия равна $p_{ok} = 1 - \cos\eta$, а для BB84 эта вероятность равна половине. В следующих строках описывается атака разбиения числа фотонов на Еву. В слабой схеме кодирования импульсов этот протокол явно небезопасен. То, что Ева может просто сделать, — это выполнить такое же однозначное измерение, как и Боб. Когда будет найден окончательный результат, она узнает состояние, и она подготовит его копию со стороны Боба. Когда Ева не может определить состояние, она блокирует пульс. Конечно, как только у нас есть некоторые потери в канале, Алиса и Боб не могут обнаружить подслушивание (так как они предполагают, что отсутствие

сигнала связано с потерями), а протокол небезопасен. Обратите внимание, что в этом случае Ева не нуждается в квантовой памяти и канале без потерь.

Рассмотрим протокол 4+2. Третий протокол распространения квантового ключа был предложен, комбинируя некоторые идеи схем B92 и BB84. Как и в протоколе BB84, есть четыре состояния, сгруппированные в два набора: $\{|0_a\rangle, |1_a\rangle\}, \{|0_b\rangle, |1_b\rangle\}$. Однако, как и в B92, состояния в каждом наборе не ортогональны, их перекрытия равны $|\langle 0_a|\, 1_a\rangle| = |\langle 0_b|\, 1_b\rangle| = \cos\eta$. Ситуация изображена на рис. 9, четыре состояния лежат на одной параллели блоховской сферы. Таким образом, Алиса выбирает случайным образом, в каком из двух наборов бит кодируется. Боб произвольно выполняет одну из двух POVM, различающих два состояния каждого набора. После согласования базиса они определяют все случаи, когда Боб применил правильные измерения, получив окончательный результат. На первый взгляд, этот протокол кажется более устойчивым к атакам с расщеплением числа фотонов: по сравнению с случаем BB84, Ева может хранить некоторые фотоны, но её измерение после примирения баз не может быть окончательным. И по сравнению с B92, она не знает, какое из двух измерений должно быть применено. Однако из-за особой геометрии множеств состояний эта схема не даёт никакого преимущества по сравнению с двумя предыдущими. Но прежде чем описывать атаку Евы, давайте покажем, как трёхмерный результат, описанный в (37), можно интерпретировать как конкатенацию двух измерений двух результатов.

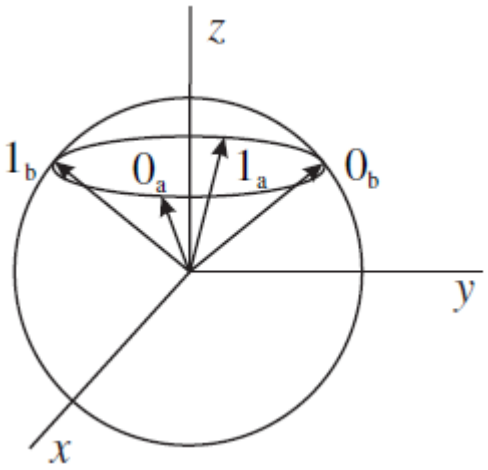

Рис. 9. Набор состояний, необходимых для протокола $4+2$.

Эффект любого квантового измерения может быть представлен набором операторов $\{A_i\}$, удовлетворяющих $\sum_i A_i A_i^\dagger =$. Если начальное состояние ρ, вероятность любого результата, скажем, i, равна

$$p_i = \mathrm{tr}\left(A_i \rho A_i^\dagger\right), \tag{38}$$

и состояние превращается в

$$\rho_i = \frac{1}{p_i} A_i \rho A_i^\dagger . \tag{39}$$

Рассмотрим состояния POVM, описываемый операторами (37), может быть эффективно заменен последовательностью двух измерений с двумя результатами. Во-первых, применяется измерение, описанное операторами

$$\begin{aligned} A_{ok} &\equiv \frac{1}{\sqrt{1+\cos\eta}} \left(|+x\rangle \langle \psi_1^\perp| + |-x\rangle \langle \psi_0^\perp|\right) \\ A_1 &\equiv \sqrt{-A_{ok} A_{ok}^\dagger} . \end{aligned} \tag{40}$$

Эффект этого первого измерения заключается в следующем: с вероятностью $p_{ok} = 1-\cos\eta$ состояние $|\psi_0\rangle$ ($|\psi_1\rangle$) отображается в $|+x\rangle$ ($|-x\rangle$). Эта операция часто называется фильтрацией, и она эквивалентна случаям, когда уравнение (37) даёт окончательный результат. Когда результат *ok* получен, говорят, что состояния прошли фильтр. Если это так, то для различения двух состояний достаточно стандартного измерения фон Неймана на основе x.

Вернемся к протоколу $4+2$ и рассмотрим фильтр для состояний в множестве a, отправляя это состояние в базу x. Нетрудно видеть, что один и тот же фильтр отображает состояния из множества b в $|\pm y\rangle$. Таким образом, BB84-подобная ситуация восстанавливается.

Теперь легко спроектировать атаку на разделение числа фотонов.

Во-первых, Ева считает количество фотонов. Как и в случае с B92, она применяет фильтрацию результатов двух исходов при получении многофотонного импульса. Когда результат является окончательным, она подаёт полученный фотон в квантовую память и передает остальную часть фотонов Бобу. Затем, как и в случае с протоколом BB84, она ждет примирения базиса и выполняет правильное измерение фон Неймана, позволяя ей прочитать бит. Для справедливого сравнения всегда применяем тот же ключ при отсутствии Евы, как в BB84, используя $\mu = 0.1$. В этом случае это означает, что должны иметь

$$\mu_{BB84} = \mu_{4+2}(1-\cos\eta)\ . \tag{41}$$

Аналогичным образом, как и выше для случая BB84, можно вычислить информацию Евы для этой атаки. Он почти совпадает с найденным для протокола BB84, а критическое расстояние опять равно $\delta_c = 52\,$км (см. рис. 8). Действительно, критическое расстояние оказывается совершенно независимым от степени неортогональности между состояниями в протоколе $4+2$, если наложить равенство исходных скоростей (41). Анализ протокола $4+2$ завершает данный раздел. Все изученные схемы распределения квантовых ключей не гарантируют безопасную передачу ключа, когда ослабление канала составляет около 15 дБ. К сожалению, использование неортогональных состояний недостаточно для избежания атак Евы. Критическое расстояние в основном соответствует точке, где скорость передачи со стороны Боба может быть имитирована числом многофотонных импульсов, покидающих лабораторию Алисы.

Проведём численные расчёты физических характеристик квантового канала связи. В работе предложена теория квантовых эффектов для описания процессов передачи и переноса квантовой информации между двумя или несколькими пользователями квантовой сети. Обсудим физические аспекты различных систем квантовой криптографии. В настоящее время в связи с возрастающими объёмами передаваемой оптической информации по телекоммуникационным и компьютерным сетям становится актуальной проблема создания новых криптосистем для кодирования информации. Привлекательность использования оптических методов передачи информации состоит в высоком быстродействии и пропускной способности оптических каналов связи, совершенных оптических методах приёма, обработки, хранения, преобразования, шифрования когерентной оптической информации. Современные системы передачи информации основаны на быстродействующих оптоволоконных линиях связи. Поэтому представляется перспективным разрабатывать оптические схемы кодирования не только классической, но и квантовой информации.

Рассмотрим методы численных расчётов характеристик квантовых криптосистем. Рассмотрим численные решения моделей для шифрования квантовой информации при переносе информации на большие расстояния между системами. На рис. 10 представлена зависимость длины линии L_c симметричного бинарного канала связи от среднего числа фотонов μ в когерентном состоянии, начиная с которых Ева может блокировать

посылки.

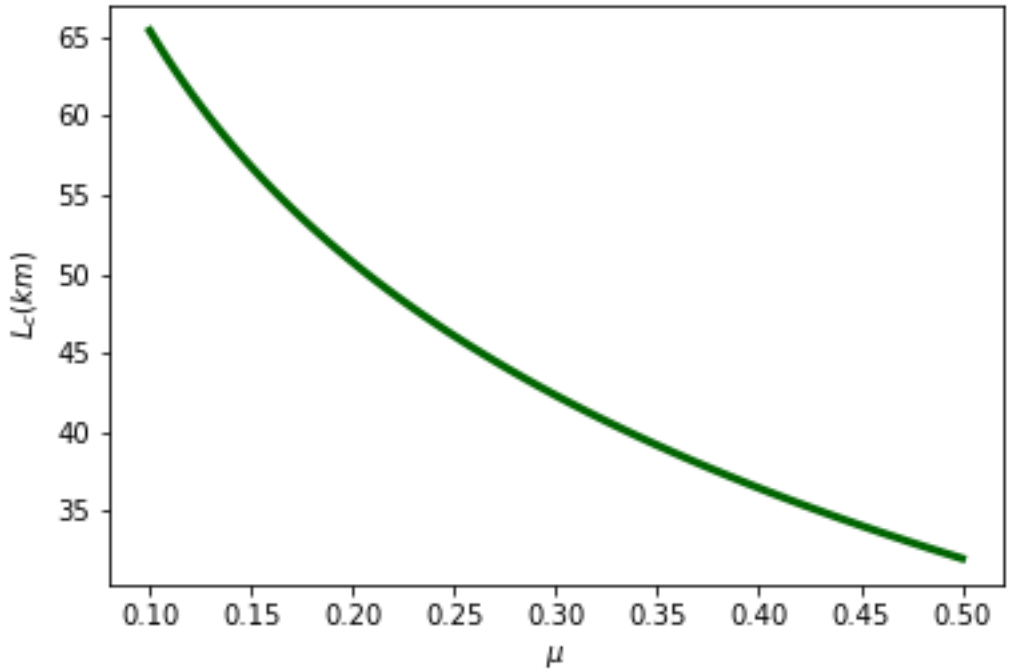

Рис. 10. Зависимость длины линии L_c симметричного бинарного канала связи от среднего числа фотонов μ, начиная с которых Ева может блокировать посылки.

На рис. 11 представлена зависимость длины линии L_k от среднего числа фотонов μ в когерентном состоянии, начиная с которых Ева может блокировать посылки, содержащие k фотонов.

На рис. 12 представлена зависимость $I(A;B)$ от длины линии связи L. Вероятности темновых отсчётов равны a) $p_{dark} = 1.0 \cdot 10^{-5}$, b) $p_{dark} = 1.0 \cdot 10^{-7}$, c) $p_{dark} = 1.0 \cdot 10^{-8}$, d) $p_{dark} = 1.0 \cdot 10^{-12}$. Квантовая эффективность фотодетекторов и среднее число фотонов в когерентном состоянии одинаковы для всех кривых и равны соответственно $\eta = 0.1$, $\mu = 0.2$. Угол между состояниями $\alpha = \pi/8$.

На рис. 13 представлены зависимости $I(A;B)$, $I(A;E)$, $I(A;B) - I(A;E)$ от длины линии связи L. Вероятности темновых отсчётов равны a) $p_{dark} = 0.85 \cdot 10^{-5}$, b) $p_{dark} = 0.85 \cdot 10^{-7}$, c) $p_{dark} = 0.85 \cdot 10^{-8}$, d) $p_{dark} = 0.85 \cdot 10^{-10}$. Квантовая эффективность фотодетекторов и среднее число фотонов в когерентном состоянии одинаковы для всех кривых и равны соответственно $\eta = 0.1$, $\mu = 0.2$. Угол между состояниями $\alpha = \pi/8$.

В основе различных схем переноса квантовой информации между квантовыми системами лежит возможность переноса квантового волнового пакета. Для переноса квантовой информации вначале необходимо создать квантовый канал связи между двумя тождественными квантовыми системами (атомами или фотонами). Затем с помощью некоторой последовательности квантовых процессов, которые возможно протекают одновременно, происходит перенос квантовой информации. Физический быстропротекающий процесс можно использовать для переноса информации с быстро исчезающих носителей (например, фотонов) на частицы более удобные для хранения информации (ионы).

Физический процесс квантовой коммуникации представляет собой совокупность квантовых эффектов кодирования, переноса и декодирования квантовой информации между двумя тождественными системами.

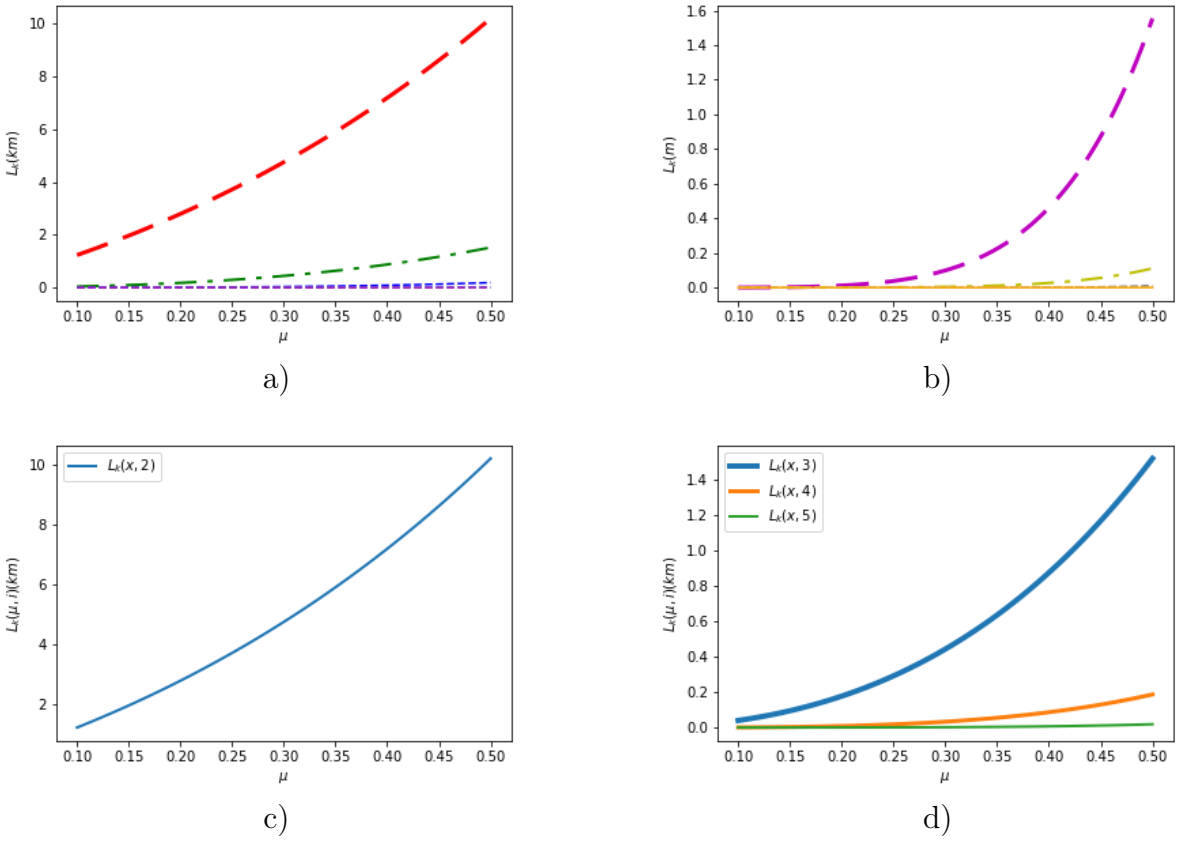

Рис. 11. Зависимость длины линии L_k от среднего числа фотонов μ в когерентном состоянии, начиная с которых Ева может блокировать посылки, содержащие k фотонов. a) $L_k(\mu, 2)$, $L_k(\mu, 3)$, $L_k(\mu, 4)$, $L_k(\mu, 5)$, b) $L_k(\mu, 6)$, $L_k(\mu, 7)$, $L_k(\mu, 8)$, $L_k(\mu, 9)$, c) $L_k(\mu, 2)$, d) $L_k(\mu, 3)$, $L_k(\mu, 4)$, $L_k(\mu, 5)$.

Заключение

В работе рассматривались основы разработки дистанционных курсов на примере дистанционного курса по физическим основам квантовой криптографии. Рассмотрены аспекты создания и применения электронных образовательных ресурсов по квантовой криптографии.

В качестве подтверждения гипотезы исследования спроектирован дистанционный курс по физическим основам квантовой криптографии, позволяющий проводить обучение основам квантовой криптографии по традиционной, смешанной и дистанционной формам обучения с применением компьютеров.

В работе построена теоретическая модель квантового канала связи. Простейшим эффектом квантовой связи является передача квантовых состояний. Для того чтобы передавать квантовые состояния атомных систем необходимо рассчитать вероятности квантовых состояний электрона в атоме при различных значениях квантовых чисел. Рассмотрены различные виды защиты от атак с расщеплением числа фотонов. Выполнены численные расчёты зависимости длины линии связи от среднего числа фотонов в когерентном состоянии, начиная с которых Ева может блокировать посылки, содержащие фиксированное число фотонов. В работе составлена компьютерная программа для расчёта характеристик секретного квантового канала связи. Исследованы оптические характеристики квантового канала в зависимости от типа канала и начальных состояний передающей и принимающей систем.

Безоговорочная безопасность систем квантовой криптографии основана на некото-

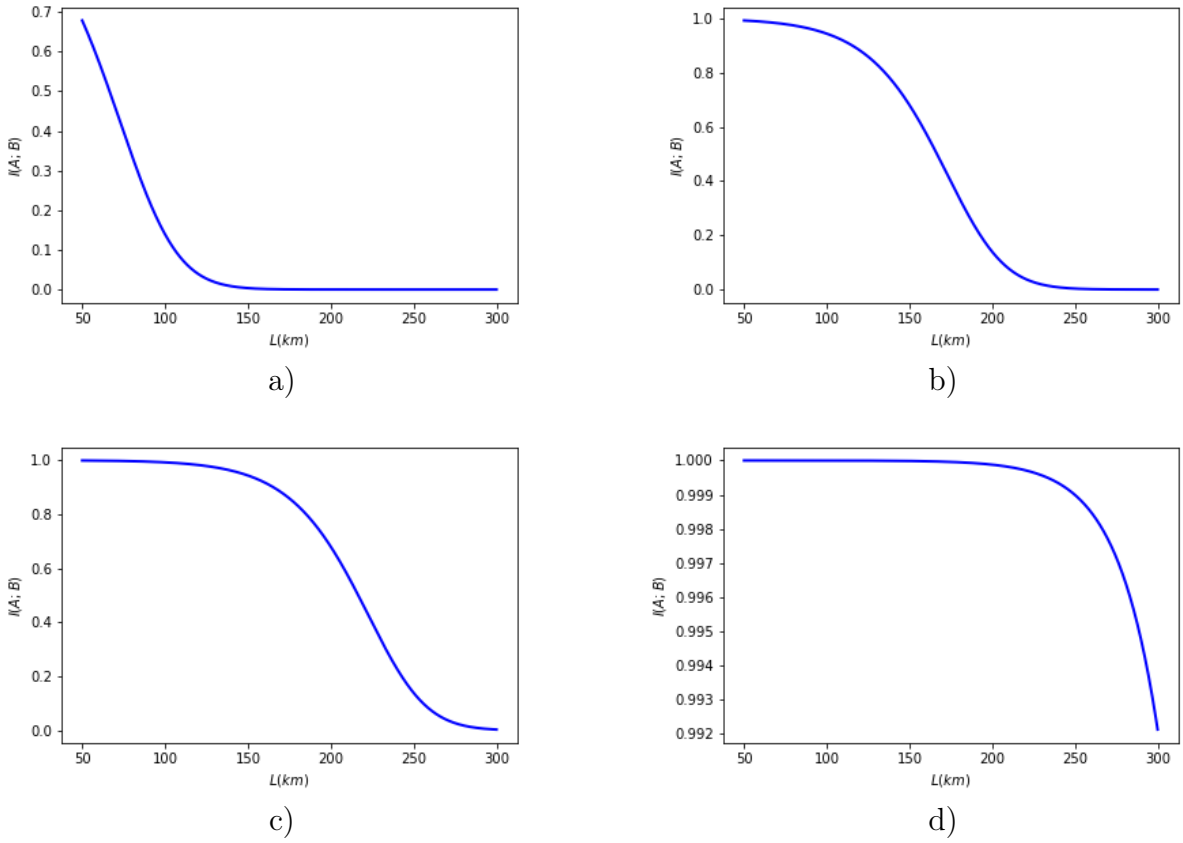

Рис. 12. Зависимость $I(A;B)$ от длины линии связи L. Вероятности темновых отсчётов равны a) $p_{dark} = 1.0 \cdot 10^{-5}$, b) $p_{dark} = 1.0 \cdot 10^{-7}$, c) $p_{dark} = 1.0 \cdot 10^{-8}$, d) $p_{dark} = 1.0 \cdot 10^{-12}$. Квантовая эффективность фотодетекторов и среднее число фотонов в когерентном состоянии одинаковы для всех кривых и равны соответственно $\eta = 0.1$, $\mu = 0.2$. Угол между состояниями $\alpha = \pi/8$.

рых экспериментальных предположениях, которые не могут быть достигнуты с помощью современной технологии. Таким образом, в более реалистичном сценарии честным сторонам приходится иметь дело с аппроксимированными однофотонными источниками, шумными каналами, неэффективными детекторами и т. д. При этом никаких ограничений на технологию прослушивания не следует принимать. Это открывает возможность для альтернативных атак с перехватом, используя технологические недостатки Алисы и Боба. Действительно, используя в качестве эталона схему BB84 с $\mu = 0.1$, все известные протоколы становятся небезопасными против атак с расщеплением числа фотонов при потерях в канале порядка 13 дБ.

Рассматривали протоколы распределения квантовых ключей, устойчивые к атакам с расщеплением числа фотонов, вплоть до потерь в канале 40 дБ. Есть два возможности для этого: 1) использовать неортогональность квантовых состояний по-другому, как в представленном протоколе с четырьмя состояниями, или 2) включить сильный опорный импульс, который должен быть всегда обнаружен Бобом. Обе возможности кажутся достижимыми с помощью современной технологии. В первом случае уже существующие реализации протокола BB84 обеспечивают экспериментальную демонстрацию защиты квантового ключа от атак с расщеплением числа фотонов, когда применяется альтернативный процесс отсеивания. Вторая возможность показывает связь между схемами распределения квантовых ключей с дискретными и непрерывными переменными, которые заслуживают дальнейшего изучения.

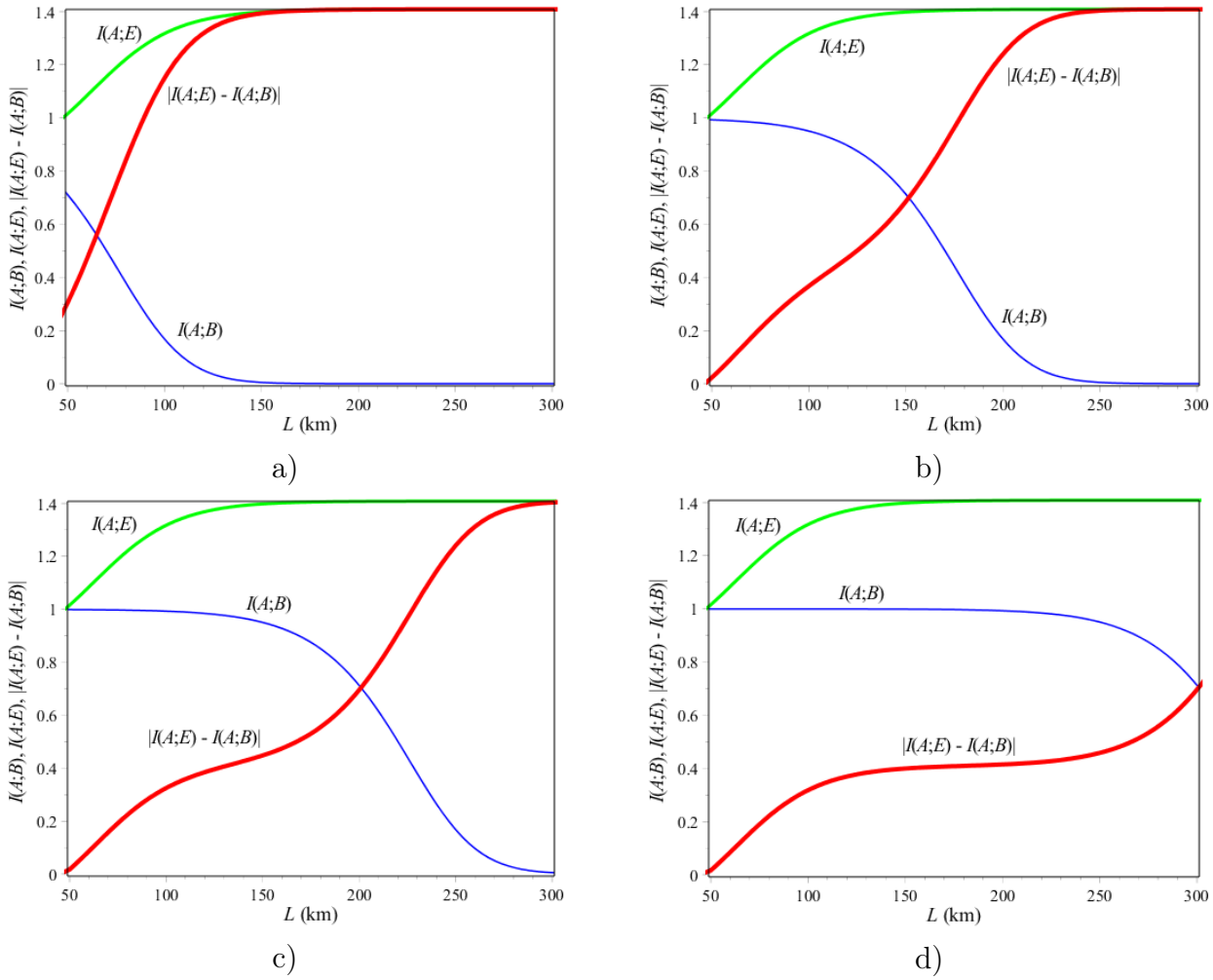

Рис. 13. Зависимости $I(A;B)$, $I(A;E)$, $I(A;B) - I(A;E)$ от длины линии связи L. Вероятности темновых отсчётов равны a) $p_{dark} = 0.85 \cdot 10^{-5}$, b) $p_{dark} = 0.85 \cdot 10^{-7}$, c) $p_{dark} = 0.85 \cdot 10^{-8}$, d) $p_{dark} = 0.85 \cdot 10^{-10}$. Квантовая эффективность фотодетекторов и среднее число фотонов в когерентном состоянии одинаковы для всех кривых и равны соответственно $\eta = 0.1$, $\mu = 0.2$. Угол между состояниями $\alpha = \pi/8$.

Рассчитаны характеристики квантового канала связи. Вычисления произведены при различных сценариях. При помощи управления переходами между квантовыми состояниями системы предложен протокол квантовой криптографии.

Наконец, очень важно, что в ходе исследований задач квантовых вычислений подвергаются новому анализу и экспериментальной проверке основные проблемы квантовой физики: проблемы локальности, реальности, дополнительности, скрытых параметров, коллапса волновой функции.

По результатам работы можно сформулировать следующие выводы:

1. проведённый анализ научной литературы по состоянию работ по квантовой криптографии показал существование возрастающих потребностей в создании дистанционных курсов по квантовой криптографии для различных уровней образования,
2. разработанная теория квантовой криптографии позволила создать и наполнить структуру лекционного курса по физическим основам квантовой криптографии,
3. разработан курс по физическим основам квантовой криптографии в системе управления обучением MOODLE, который готов к использованию в учебном процессе в качестве дистанционного курса или курса по смешанной технологии обучения.

Показано, что эффективность кодирования квантовой информации можно увеличить, если использовать эффект квантового сжатия фотонных состояний. Произведена оценка вероятности подслушивания при передаче квантовой информации в оптической сети между взаимодействующими атомами, помещёнными в общее поле фотонов. Показана принципиальная возможность создания квантового алгоритма переноса квантовой информации, защищённого от возможности прослушивания.

Использование дистанционного курса по физическим основам квантовой криптографии, созданного в системе управления обучением MOODLE, способствует интенсификации учебного процесса и более осмысленному изучению материала, приобретению навыков самоорганизации и превращению систематических знаний в системные, помогает развитию познавательной деятельности студентов и интереса к предмету.

Созданный в работе дистанционный курс по физическим основам квантовой криптографии, созданный в системе управления обучением MOODLE на образовательном портале университета, позволяет эффективно планировать, организовывать и проводить обучение по квантовой криптографии в педагогическом университете.

Список использованных источников

1. Quantum cryptography / N. Gisin [et al.] // Reviews of Modern Physics. — 2002. — mar. — Vol. 74, no. 1. — P. 145–195. — URL: https://doi.org/10.1103/revmodphys.74.145.

2. Wootters W. K., Zurek W. H. A single quantum cannot be cloned // Nature. — 1982. — oct. — Vol. 299, no. 5886. — P. 802–803. — URL: https://doi.org/10.1038/299802a0.

3. Ekert A. K. Quantum cryptography based on Bell's theorem // Physical Review Letters. — 1991. — aug. — Vol. 67, no. 6. — P. 661–663. — URL: https://doi.org/10.1103/physrevlett.67.661.

4. Elliott Ch. Building the quantum network // New Journal of Physics. — 2002. — jul. — Vol. 4. — P. 46–46. — URL: https://doi.org/10.1088/1367-2630/4/1/346.

5. Wang Y. Unconditional Security of Cryptosystem: A Review and Outlook // Trends in Applied Sciences Research. — 2011. — jun. — Vol. 6, no. 6. — P. 554–562. — URL: https://doi.org/10.3923/tasr.2011.554.562.

6. Security of Quantum Key Distribution Usingd-Level Systems / N. J. Cerf [et al.] // Physical Review Letters. — 2002. — mar. — Vol. 88, no. 12. — URL: https://doi.org/10.1103/physrevlett.88.127902.

7. Molotkov S. N. What is a quantum cryptography protocol that ensures the maximum distance in the case of a strictly single-photon source? // JETP Letters. — 2015. — oct. — Vol. 102, no. 7. — P. 473–477. — URL: https://doi.org/10.1134/s0021364015190108.

8. Molotkov S. N. On the stability of fiber-optic quantum cryptography at arbitrary losses in a communication channel: Exclusion of unambiguous measurements // JETP Letters. — 2014. — nov. — Vol. 100, no. 6. — P. 413–419. — URL: https://doi.org/10.1134/s0021364014180076.

9. Molotkov S. N. Relativistic quantum cryptography on "Arrested" photons // Journal of Experimental and Theoretical Physics Letters. — 2002. — jul. — Vol. 76, no. 1. — P. 71–76. — URL: https://doi.org/10.1134/1.1507231.

10. Molotkov S. N., Potapova T. A. Wavefunctions of a prolate spheroid and multiplexing in relativistic quantum cryptography on orthogonal states // JETP Letters. — 2015. — jan. — Vol. 100, no. 9. — P. 596–603. — URL: https://doi.org/10.1134/s0021364014210115.

11. Molotkov S. N. On the quantum-mechanical bound on the loss of information through side channels in quantum cryptography // JETP Letters. — 2013. — jul. — Vol. 97, no. 10. — P. 604–610. — URL: https://doi.org/10.1134/s002136401310007x.

12. Molotkov S. N. Relativistic quantum cryptography for open space without clock synchronization on the receiver and transmitter sides // JETP Letters. — 2011. — nov. — Vol. 94, no. 6. — P. 469–476. — URL: https://doi.org/10.1134/s0021364011180093.

13. Molotkov S. N., Nazin S. S. Quantum cryptography based on homodyne detection (vacuum-state cryptosystem) // Journal of Experimental and Theoretical Physics Letters. — 1997. — jul. — Vol. 66, no. 1. — P. 68–72. — URL: https://doi.org/10.1134/1.567485.

14. Molotkov S. N. On the ultimate capabilities of the quantum key distribution with the control over the statistics of a non-single-photon source // JETP Letters. — 2008. — jul. — Vol. 87, no. 10. — P. 586–591. — URL: https://doi.org/10.1134/s0021364008100159.

15. Bennett Ch. H., Brassard G. Quantum public key distribution reinvented // ACM SIGACT News. — 1987. — jul. — Vol. 18, no. 4. — P. 51–53. — URL: https://doi.org/10.1145/36068.36070.

16. Plesch M., Pawłowski M., Pivoluska M. 1-out-of-2 oblivious transfer using a flawed bit-string quantum protocol // Physical Review A. — 2017. — apr. — Vol. 95, no. 4. — URL: https://doi.org/10.1103/physreva.95.042324.

17. Kronberg D. A., Molotkov S. N. Quantum key distribution in a single-photon regime with nonorthogonal basis states // JETP Letters. — 2009. — jun. — Vol. 89, no. 7. — P. 370–376. — URL: https://doi.org/10.1134/s0021364009070133.

18. Kronberg D. A., Molotkov S. N. Enhancement of the robustness of phase-time quantum cryptography by block error correction // JETP Letters. — 2010. — oct. — Vol. 92, no. 7. — P. 490–495. — URL: https://doi.org/10.1134/s0021364010190124.

Сведения об авторах:

Яна Сергеевна Замлелова — магистрант факультета физико-математического и технологического образования ФГБОУ ВО «Ульяновский государственный педагогический университет имени И. Н. Ульянова», Ульяновск, Россия.

E-mail: zamlelowa1998@mail.ru

ORCID iD 0000-0002-6761-5478

Web of Science ResearcherID ABA-5168-2020

Development of elements of a distance course on the physical foundations of quantum cryptography

Ya. S. Zamlelova

Ulyanovsk State Pedagogical University, 432071, Ulyanovsk, Russia

Submitted March 18, 2021
Resubmitted April 14, 2021
Published June 12, 2021

Abstract. The description of the development of elements of an online course on the physical foundations of quantum cryptography using the MOODLE toolkit is made. An online course on elementary physics, created using the MOODLE toolkit, can be used to inform students' blended learning when studying the physical foundations of quantum cryptography, as well as to visualize the process of learning the physical foundations of quantum cryptography. The use of course control elements on the physical foundations of quantum cryptography will make it possible to systematize the control of theoretical knowledge on the physical foundations of quantum cryptography.

Keywords: course, quantum cryptography, physical foundations of quantum cryptography, pedagogical education, informatization of education, university educational process, distance learning methods

PACS: 03.67.Dd

References

1. Plesch M., Pawłowski M., Pivoluska M. 1-out-of-2 oblivious transfer using a flawed bit-string quantum protocol // Physical Review A. — 2017. — apr. — Vol. 95, no. 4. — URL: https://doi.org/10.1103/physreva.95.042324.

2. Ekert A. K. Quantum cryptography based on Bell's theorem // Physical Review Letters. — 1991. — aug. — Vol. 67, no. 6. — P. 661–663. — URL: https://doi.org/10.1103/physrevlett.67.661.

3. Elliott Ch. Building the quantum network // New Journal of Physics. — 2002. — jul. — Vol. 4. — P. 46–46. — URL: https://doi.org/10.1088/1367-2630/4/1/346.

4. Wang Y. Unconditional Security of Cryptosystem: A Review and Outlook // Trends in Applied Sciences Research. — 2011. — jun. — Vol. 6, no. 6. — P. 554–562. — URL: https://doi.org/10.3923/tasr.2011.554.562.

5. Quantum cryptography / N. Gisin [et al.] // Reviews of Modern Physics. — 2002. — mar. — Vol. 74, no. 1. — P. 145–195. — URL: https://doi.org/10.1103/revmodphys.74.145.

6. Wootters W. K., Zurek W. H. A single quantum cannot be cloned // Nature. — 1982. — oct. — Vol. 299, no. 5886. — P. 802–803. — URL: https://doi.org/10.1038/299802a0.

7. Security of Quantum Key Distribution Usingd-Level Systems / N. J. Cerf [et al.] // Physical Review Letters. — 2002. — mar. — Vol. 88, no. 12. — URL: https://doi.org/10.1103/physrevlett.88.127902.

8. Bennett Ch. H., Brassard G. Quantum public key distribution reinvented // ACM SIGACT News. — 1987. — jul. — Vol. 18, no. 4. — P. 51–53. — URL: https://doi.org/10.1145/36068.36070.

9. Molotkov S. N. On the ultimate capabilities of the quantum key distribution with the control over the statistics of a non-single-photon source // JETP Letters. — 2008. — jul. — Vol. 87, no. 10. — P. 586–591. — URL: https://doi.org/10.1134/s0021364008100159.

10. Kronberg D. A., Molotkov S. N. Quantum key distribution in a single-photon regime with nonorthogonal basis states // JETP Letters. — 2009. — jun. — Vol. 89, no. 7. — P. 370–376. — URL: https://doi.org/10.1134/s0021364009070133.

11. Kronberg D. A., Molotkov S. N. Enhancement of the robustness of phase-time quantum cryptography by block error correction // JETP Letters. — 2010. — oct. — Vol. 92, no. 7. — P. 490–495. — URL: https://doi.org/10.1134/s0021364010190124.

12. Molotkov S. N. What is a quantum cryptography protocol that ensures the maximum distance in the case of a strictly single-photon source? // JETP Letters. — 2015. — oct. — Vol. 102, no. 7. — P. 473–477. — URL: https://doi.org/10.1134/s0021364015190108.

13. Molotkov S. N. On the stability of fiber-optic quantum cryptography at arbitrary losses in a communication channel: Exclusion of unambiguous measurements // JETP Letters. — 2014. — nov. — Vol. 100, no. 6. — P. 413–419. — URL: https://doi.org/10.1134/s0021364014180076.

14. Molotkov S. N. Relativistic quantum cryptography on “Arrested” photons // Journal of Experimental and Theoretical Physics Letters. — 2002. — jul. — Vol. 76, no. 1. — P. 71–76. — URL: https://doi.org/10.1134/1.1507231.

15. Molotkov S. N., Potapova T. A. Wavefunctions of a prolate spheroid and multiplexing in relativistic quantum cryptography on orthogonal states // JETP Letters. — 2015. — jan. — Vol. 100, no. 9. — P. 596–603. — URL: https://doi.org/10.1134/s0021364014210115.

16. Molotkov S. N. Relativistic quantum cryptography for open space without clock synchronization on the receiver and transmitter sides // JETP Letters. — 2011. — nov. — Vol. 94, no. 6. — P. 469–476. — URL: https://doi.org/10.1134/s0021364011180093.

17. Molotkov S. N. On the quantum-mechanical bound on the loss of information through side channels in quantum cryptography // JETP Letters. — 2013. — jul. — Vol. 97, no. 10. — P. 604–610. — URL: https://doi.org/10.1134/s002136401310007x.

18. Molotkov S. N., Nazin S. S. Quantum cryptography based on homodyne detection (vacuum-state cryptosystem) // Journal of Experimental and Theoretical Physics Letters. — 1997. — jul. — Vol. 66, no. 1. — P. 68–72. — URL: https://doi.org/10.1134/1.567485.

Information about authors:

Yana Sergeevna Zamlelova — Master's student of the Faculty of Physics, Mathematics and Technological Education of the Ulyanovsk State Pedagogical University, Ulyanovsk, Russia.

E-mail: zamlelowa1998@mail.ru
ORCID iD 0000-0002-6761-5478
Web of Science ResearcherID ABA-5168-2020