Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

УДК 004.056.53:003.26:621.39:530.145:535.14 На правах рукописи

ЮБУЗОВА ХАЛИЧА ИБРАГИМОВНА

Методы безопасного распределения ключей на базе протоколов квантовой криптографии

6D070400 – Вычислительная техника и программное обеспечение

Диссертация на соискание степени
доктора философии (PhD)

Научный консультант:
Ахметов Б.С.
д.т.н., профессор

Научный консультант:
Гнатюк С.А.
д.т.н., профессор, зам. декана ф-та Кибербезопасности компьютерной программной инженерии Национального авиационного университета (Украина)

Республика Казахстан
Алматы, 2022

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В данной диссертации использованы ссылки на следующие стандарты:

ГОСО РК 5.04.034-2011 «Государственный общеобязательный стандарт образования Республики Казахстан. Послевузовское образование. Докторантура. Основные положения» (изменения от 23 августа 2012 г. № 1080);

Положение о диссертационном совете НАО «КазНИТУ имени К.И.Сатпаева». П 029-04-01.01 - 2021

Правила присуждения ученых степеней от 31 марта 2011 года № 127;

Межгосударственные стандарты:

ГОСТ 7.32-2001 (изменения от 2006 г.). Отчет о научно-исследовательской работе. Структура и правила оформления;

ГОСТ 7.1-2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления.

Закон Республики Казахстан «О науке» от 18.02.2011 г. № 407-IV ЗРК;

Правила, разработанные в АО «Национальный центр научно-технической информации» в 2014 году

«Инструкция по диссертации и абстрактным тезисам», МОН РК, Высшая аттестационная комиссия, Алматы, 2004 год.

СТ РК 34.007-2002. Информационные технологии. Телекоммуникационные сети. Основные термины и определения.

ОПРЕДЕЛЕНИЯ

В настоящей диссертации применяются следующие термины и соответствующие определения:

Базис Белла – набор ортогональных состояний кубитов (кудитов) при использовании квантовой корреляции.

Гильбертово пространство – обобщение евклидова пространства, допускающее бесконечную размерность.

Детерминистический протокол – асимптотически стойкий протокол квантовой криптографии, который базируется на эффекте квантовой корреляции.

Квант – элементарная неделимая порция физической величины, которая является носителем некоторого типа взаимодействия (например, фотон, фонон, электрон, гравитон). В диссертации в качестве квантов используются фотоны.

Квантовая корреляция – квантово-механическое явление, при котором квантовые состояния двух или большего числа объектов оказываются взаимозависимыми.

Квантовая криптография – метод защиты коммуникаций, основанный на принципах квантовой физики и квантовой механики. Для передачи информации применяются объекты физических средств, такие как электроны в электрическом токе, или фотоны в линиях волоконно-оптической связи.

Квантовые протоколы – оговоренные априори правила передачи информации между двумя легитимными пользователями с использованием закодированных состояний фотонов.

Кварт – логарифмическая единица измерения в теории информации, минимальная целая единица измерения количества информации источников с четырьмя равновероятными сообщениями.

Клонирование – создание точных копий (клонов) какого-либо объекта.

Когерентное состояние – характеристика суперпозиции, для которой существует базис, в котором значение кубита (кудита) строго определено.

Кубит – квантовый разряд или наименьший элемент для хранения информации в квантовом компьютере (принимает значение $|0\rangle$ или $|1\rangle$).

Кудит – *d*-уровневая система, которая является обобщением понятия кубит на многоуровневые квантовые системы.

Кукварт – квантовая ячейка, имеющая четыре возможных состояния: $|0\rangle$, $|1\rangle, |2\rangle, |3\rangle$.

Кутрит – квантовая ячейка, имеющая три возможных состояния: $|0\rangle, |1\rangle, |2\rangle$.

Некогерентная атака – метод перехвата (снятия) информации в квантовой криптографии, который заключается в перехвате информации нарушителем с использованием дополнительных квантовых систем (проб).

Ортогональность – обобщение перпендикулярности для линейных пространств, при котором скалярное произведение двух векторов равно нулю.

Поляризация – тип кодирования в квантовой криптографии, когда классическая информация кодируется с использованием углов поляризации фотонов.

Постулат квантовой механики – принципиальное утверждение, которое характерно в квантовой физики и на незыблемости которого базируется стойкость квантовой криптографии.

Синглетное поляризационное состояние (синглет) – перепутанное состояние двух квантовых частиц, при котором их суммарный спин равен нулю.

Спин – собственный момент импульса элементарных частиц, имеющий квантовую природу и не связанный с перемещением частицы как целого.

Суперпозиция – базисное состояния кубита, при котором невозможно утверждать с определенностью, что кубит находится в состоянии $|0\rangle$ или $|1\rangle$, т.е. он находится в состоянии $|\Psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ в некоторый момент времени.

Теорема о запрете клонирования – утверждение квантовой теории о невозможности создания идеальной копии произвольного неизвестного квантового состояния.

Трит – логарифмическая единица измерения в теории информации, минимальная целая единица измерения количества информации источников с тремя равновероятными сообщениями.

Фотон – квант электромагнитного поля, элементарная нейтральная частица, которая является носителем электромагнитного взаимодействия.

Энтропия Холево – ограниченное количество классической информации, которую можно получить в результате квантового измерения.

Эрмитово сопряженный вектор – состояние векторов $\langle\ |$ и $|\ \rangle$ («бра» и «кет») в гильбертовом пространстве.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

GF(3) – поле Галуа (конечное поле) размером (диапазоном до) 3.

$\langle$ | и | $\rangle$ – «бра» и «кет», обозначение векторов состояний в гильбертовом пространстве.

ИКС – Информационно-Коммуникационные системы

ИКТ – Информационно-Коммуникационные технологии

КК – Квантовая криптография

ЭПР-пара – состояние Эйнштейна-Подольского-Розена (для пары фотонов)

ГХЦ – Гринбергера-Хорна-Цайлингера состояние (для n фотонов)

КЦП – Квантовая цифровая подпись

КПРК – Квантовые протоколы распределения ключа

КПШ – Квантовый потоковый шифр

КПРС – Квантовый протокол разделения секрета

КППБС – Квантовые протоколы прямой безопасной связи

ЗИ – Защита информации

ККМ – Квантовые криптографические методы

КРК – Квантовое распределение ключей

ПСЧП – Псевдослучайные последовательности

КТ – Квантовая телепортация

КС – Квантовая стеганография

КРС – Квантовое разделение секрета (quantum secret sharing, QSS)

КПБС – Квантовая прямая безопасная связь

КРК с дискретными переменными DV-QKD (discrete-variable);

КРК с непрерывными переменными CV-QKD (continuous-variable);

ПСП – Протоколы с состояниями «приманки» (decoy states protocols);

КВБ – Квантовое вручение бита (quantum bit commitment);

КПМ – Квантовое подбрасывание монеты (quantum coin tossing);

КР – Квантовая рулетка (quantum gambling).

МПИ – Методы перехвата информации

НСД – Несанкционированный доступ

РС-коды – Коды Рида Соломона

КДП – Квантовый детерминистический протокол

ДПК – Деполяризующий канал

RSA – Rivest Shamir Adleman (ассиметричный алгоритм шифрования)

DES – Data Encryption Standard (стандарт шифрования США)

AES – Advanced Encryption Standard (стандарт шифрования США)

BB84 – Bennet Brassard 1984 (первый квантовый протокол)

SSL – Secure Sockets Layer, уровень защищенных сокетов.

IBM – International Business Machines Corp, американская корпорация, которая является мировым лидером по разработке компьютеров и вычислительных технологий.

B92 – Квантовый протокол Беннета 1992 года

E91 – Квантовый протокол Экерта 1991 года

SARG04 – Квантовый протокол распределения ключей

QPN – quantum private network

MagiQ Technologies – Американская компания, которая занимается разработкой коммерческих квантово-криптографических систем

Id Quantique – Швейцарская компания – мировой лидер по разработке коммерческих квантово-криптографических систем

QinetiQ – Британская компания, которая занимается разработкой коммерческих квантово-криптографических систем

PNS attack – (Photon number splitting attack) атаки разделения числа фотонов

PBS attack – (Photon beam splitting attack) атаки разделения пучка фотонов

TriGen – Генератор троичных псевдослучайных последовательностей

ВВЕДЕНИЕ

Оценка современного состояния решаемой научной или научно технологической проблемы

Анализ состояния и мониторинг проблемы обеспечения конфиденциальности передачи данных в современных информационных и коммуникационных системах (ИКС) показывает, что одним из основных методов является применение криптографии [1-4]. В настоящее время, как правило, используются методы симметричной и ассиметричной криптографии, которые имеют определенные недостатки. Например, симметричные криптосистемы [1, с. 15, 2, с. 70] являются достаточно быстродействующими и стойкими к атакам, однако при их использовании возникает сложная проблема распределения секретных ключей. Существует несколько способов решения этой проблемы, среди которых, например, использование методов ассиметричной криптографии [3, с. 294, 4, с.135, 5] или передача ключей с помощью доверенных курьеров. Но и эти способы также обладают существенными недостатками – ассиметричные криптосистемы относительно медленные (на 2-3 порядка по сравнению с симметричными), а их криптостойкость основана на невозможности эффективного вычислительного решения NP-сложных задач (например, таких, как факторизация и логарифмирование в дискретных полях большого размера). Однако данная невозможность является гипотезой, которая в любой момент может быть опровергнута, если будет доказано противоположное ей предположение. Это может привести к краху большей части современной традиционной криптографии, так как она базируется на задачах, тесно связанных между собой. Кроме того, быстрое увеличение производительности и одновременное удешевление вычислительных средств, а также открытие новых, более эффективных алгоритмов решения некоторых NP-сложных задач (алгоритмы Шора, Гровера и т.п. [6]) делает перспективы традиционной криптографии не вполне надежными. Еще одной угрозой методам традиционной криптографии является перспектива появления устойчивых многокубитных квантовых вычислительных систем (квантовых компьютеров).

В связи с этим, большой интерес вызывает квантовая криптография (КК) [7, 8], которая использует специфические свойства квантовых систем, служащие носителями информации в протоколах КК, и дает возможность достичь при решении некоторых задач защиты информации теоретико-информационной стойкости, которая не зависит от вычислительных и других возможностей злоумышленника. За последние десятилетия КК прошла путь от лабораторных экспериментов до внедрения полноценных коммерческих решений.

Исследования отечественных и зарубежных ученых [9, 10-19] посвящены развитию теории и практики квантовой криптографии, среди них Ахметов Б., Беннет Ч., Брассар Ж., Василиу Е., Гнатюк С., Диаманти Е., Жмурко Т., Завадски П., Зеневич А., Килин С., Лам П., Люткенхаус Н., Реннер Р., Румянцев К., Холево А.С., Явич М. и др.

Основание и исходные данные для разработки темы

Основанием для разработки темы является необходимость и потребность в поиске новых методов по обеспечению конфиденциальности передачи данных по коммуникационным сетям, защиты информации и реализации концепции кибербезопасности. Целью Концепции кибербезопасности «Киберщит Казахстана» является обеспечение информационной безопасности общества и государства в сфере информатизации и связи, а также защита неприкосновенности частной жизни граждан при использовании ими информационно-коммуникационных технологий (ИКТ). Кроме этого, государственная программа «Цифровой Казахстан» декларирует, что основные проблемы и угрозы безопасности в сфере использования ИКТ, влияющие на эффективность процессов цифровизации экономики Казахстана, меры по их преодолению нашли отражение в Концепции кибербезопасности «Киберщит Казахстана» и предусматривают использование доверенных технологий обеспечения целостности, конфиденциальности, доступности информации и аутентификации пользователей при ее обработке.

Однако, создание и развитие эффективных технологий обеспечения конфиденциальности должны учитывать современные угрозы и эффективно им противодействовать в независимости от возможностей злоумышленников.

Обоснование необходимости проведения научно-исследовательской работы

Необходимость проведения настоящей научно-исследовательской работы продиктована намеченными мероприятиями Концепции кибербезопасности («Киберщит Казахстана»), разработанной в соответствии с посланием Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная конкурентоспособность». В частности, в данной Концепции в числе ключевых проблем в сфере защиты электронных информационных ресурсов указано, что «Несмотря на достигнутый высокий уровень информатизации сферы государственного управления, включая оборону и безопасность, широкое использование ИКТ в различных сферах жизни личности и общества, Казахстан как страна пока в значительной мере импортирует (заимствует) не только IT-технологии, но и готовые программные продукты, включая продукты обеспечения информационной безопасности в сфере информатизации и связи. Это указывает с одной стороны на давление со стороны гигантов IT-индустрии, а с другой на недостаточность принимаемых усилий и мер по их рациональному замещению с опорой на собственные силы в критически важных сферах разработок, от которых зависит обеспечение безопасности государства.

В связи с этим, разработка методов повышения эффективности распределения ключей шифрования на базе протоколов квантовой криптографии и дальнейшее их внедрение в существующие ИКТ инфраструктуры может позволить преодолеть упомянутые проблемы Казахстана.

Сведения о планируемом научно-техническом уровне разработки, о патентных исследованиях и выводы из них

При постановке исследований планировалась разработка методов повышения эффективности распределения ключей шифрования на базе протоколов

квантовой криптографии. Научно-технический уровень разработки соответствует современным требованиям: использован целый комплекс достаточно точных методов исследования: методы теории защиты информации, теории криптографии и криптоанализа, квантовой теории информации, квантовой механики, имитационного моделирования и др. Подтверждается использованием современных методов исследования и анализа, апробацией и научными публикациями соискателя по теме исследований.

Проведен анализ литературных данных и патентных исследований в области обеспечения методов повышения эффективности распределения ключей шифрования.

Анализ патентных исследований показал, что в направлении исследований имеется ряд запатентованных работ за рубежом. Pat. № 6438234 USA, H04L 9/08 (20060101), H04K 001/00. Quantum cryptography device and method. /Gisin, Zbinden et al – 20.08.2002; Pat. № 6748081 USA, H04L 9/08 (20060101), C09K 19/02 (20060101), G02F 1/13 (20060101). Quantum cryptography system for a secure transmission of random keys using a polarization setting method. /Dultz, Wolfgang et al – 08.06.2004; Pat. № 6895092 USA, H04L 9/08 (20060101), G06F 017/00. Cryptographic key distribution method and apparatus thereof. /Tomita, Akihisa et al – 17.05.2005; Пат. № 2302085 РФ, H04L9/00 (2006.01). Способ кодирования и передачи криптографических ключей. /Молотков С., Кулик С. – № 200513476; 16.11.2005; Пат. № 2325039 РФ, H04L9/00 (2006.01). Способ кодирования и передачи криптографических ключей. /Молотков С., Кулик С. – № 2006119652; 06.06.2006; Pat. № 7178277 USA, H04K 1/00 (20060101). Quantum cryptography communication system and quantum cryptography key distributing method used in the same. /Takeuchi, Takeshi et al – 20.02.2007; Pat. № 7266304 USA, H04B 10/00 (20060101), H04K 1/00 (20060101). System for secure optical transmission of binary code. /Duraffourg, Laurent et al – 04.09.2007; Pat. № 7461323 USA, H03M 13/00 (20060101). Quantum key delivery method and communication device. /Matsumoto, Wataru et al – 02.12.2008; Пат. № 43779 України, МПК H04L 9/08. Система передачі криптографічних ключів. /Гнатюк С.О., Кінзерявий В.М., Корченко О.Г., Паціра Є.В. – №u200904239; заявл. 29.04.2009; опубл. 25.08.2009, Бюл. №16. Однако способ, предлагаемый в дисертации, отличается от приведенных работ.

Сведения о метрологическом обеспечении диссертации

Достоверность полученных результатов подтверждается применением комплекса достаточно точных методов исследования.

Исследования проводили с использованием приборов и средств измерений, соответствующих метрологическим требованиям:

- в лабораториях Национального авиационного университета, Украина Киев;

- в лабораториях УО Белорусская государственная академия связи, Белоруссия, Минск.

Экспериментальная установка представляет собой аппаратно-программный комплекс, предназначенный для проведения исследований разработанных моделей и методов. Вычислительные возможности и конфигурация аппаратного

обеспечения экспериментальной установки определялись с позиций обеспечения минимально допустимых требований к пакету прикладных программ MATLAB. В базовой конфигурации использован универсальный персональный компьютер на основе процессора Intel(R) Core (TM) i5-4200U @ 2.30GHz с оперативной памятью объемом 5,78 ГБ, жестким диском объема 1 ТБ и сетевой картой Realtek Gigabit Ethernet.

Для генерации и передачи фотонов использовалось следующее оборудование: экспериментальная установка квантовой системы реализующий работу протокола BB84 и B92; экспериментальная установка по измерению счетных характеристик одно квантовых фотоприемников; экспериментальная установка с холодильной камерой для измерения влияния напряжения и температуры на длительности фотонов и спада регистрируемых импульсов; специализированное оборудование: оптический тестер ОТ-2-8; рефлектометр МТР 600; мобильная измерительная платформа МТР 9000А; измеритель хроматической дисперсии ИД-2-2/12 и др.

Актуальность темы

Актуальность работы связана с разработкой современных методов повышения эффективности распределения ключей шифрования на базе протоколов квантовой криптографии. Методы КК, в отличии от традиционной, не зависят от вычислительных возможностей злоумышленника и, как следствие, являются более надежными с точки зрения обеспечения конфиденциальности данных. Однако, не все протоколы КК позволяют обеспечить теоретико-информационную стойкость и высокую скорость передачи данных. Как правило, эти показатели являются взаимозависимыми и повышение уровня стойкости непременно приводит к понижению скорости обработки и передачи данных – это понижает эффективность распределения ключей шифрования в режиме реального времени. Анализ современных исследований и публикаций указывает на необходимость решения задач разработки методов повышения эффективности распределения ключей шифрования на базе протоколов квантовой криптографии, обеспечения конфиденциальности передачи данных и дальнейшего их внедрения в существующие ИКТ инфраструктуры [7, с. 9, 9, с. 229-230, 11, 18-19]. На основании вышесказанного следует, что выбор направления исследований настоящей диссертационной работы является актуальным, а результаты, полученные в ходе работы, имеют научную и практическую значимость.

Новизна темы

Новизна темы заключается в разработке и исследовании метода безопасного распределения ключей, улучшения его характеристик, а именно повышения скорости передачи и обеспечении помехоустойчивости деполяризационного квантового канала на основе использования квантового детерминистического протокола распределения ключей шифрования.

Научная новизна результатов исследования:

- на основе результатов анализа современного состояния в области квантовой криптографии и связи, выявлены недостатки существующих методов распределения ключей, расширена классификация квантово-криптографических методов,

которая позволяет расширить возможности по выбору необходимых квантово-криптографических методов для построения безопасных систем распределения ключей шифрования;

- разработана модель квантового детерминистического протокола в режиме контроля подслушивания, учитывающая особенности квантового канала и вероятности возникновения в нем ошибки, что позволяет обеспечить безопасное и быстрое распределение ключей, сформулировать практические рекомендации по разработке квантово-криптографических систем в условиях использования деполяризационного квантового канала и присутствия нарушителя;

- разработана модель квантового детерминистического протокола в режиме передачи сообщений, которая дает возможность повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом при небольшом уровне природных шумов;

- предложен метод усиления секретности с использованием квантовых перепутанных состояний и сгенерированных троичных псевдослучайных последовательностей, что позволяет повысить скорость передачи, без потерь стойкости к некогерентной атаке, детерминистических протоколов квантовой криптографии с использованием пар кутритов;

- впервые реализована комбинированная модель на основе разработанных модели режима контроля подслушивания и модели режима передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов с использованием предложенного метода усиления секретности, что позволило усовершенствовать метод безопасного распределения ключей, повысить скорость и обеспечить помехоустойчивость деполяризационного квантового канала.

Связь работы с другими научно-исследовательскими работами, государственными программами

Диссертационная работа имеет связь с научно-исследовательскими работами, выполняемыми в рамках Концепции кибербезопасности «Киберщит Казахстана». Данная концепция разработана в соответствии с Посланием Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная конкурентоспособность» с учетом подходов Стратегии «Казахстан-2050» по вхождению Казахстана в число 30-ти самых развитых государств мира. А также результаты данной работы соответствуют целям и задачам Государственной программы «Информационный Казахстан – 2020».

Кроме этого, работа связана с научно-исследовательской работой «Квантово-криптографические методы защиты критической информационной инфраструктуры государства» №161-ДБ17 (№ госрегистрации 0117U006770), которая выполнялась на протяжении 2017-2019 гг. в Национальном авиационном университете (Киев, Украина).

Цель исследований – разработка моделей безопасного распределения секретных ключей и повышение эффективности их распределения за счет использования комбинированной модели на базе протоколов квантовой криптографии.

Объект исследований – процесс распределения ключей шифрования для обеспечения конфиденциальности передачи данных в ИКС**.**

Предмет исследований – методы и модели безопасного распределения ключей на базе протоколов квантовой криптографии.

Задачи исследования, их место в выполнении научно-исследовательской работы в целом:

- провести анализ современных методов, моделей и коммерческих систем распределения ключей шифрования по критериям безопасности (защищенности) и скорости;
- разработать модель угроз и модель нарушителя в квантово-криптографических системах;
- разработать и исследовать модель квантового детерминистического протокола в режиме контроля подслушивания;
- разработать и исследовать модель квантового детерминистического протокола в режиме передачи сообщений;
- разработать комбинированную модель с режимом контроля подслушивания и режимом передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов;
- предложить новый метод безопасного распределения ключей комбинированной модели с режимом контроля подслушивания и режимом передачи сообщений квантового детерминистического протокола.

Каждая решаемая задача настоящей диссертационной работы логически связана с остальными и направлена на достижение поставленной цели исследований.

Методологическая база исследований

К числу основных методов исследования и анализа, применяемых при выполнении диссертационной работы, относятся:

- критический анализ и выбор направления исследований;
- современные научные методы анализа и исследований;
- современные методы теории защиты информации;
- теория криптографии и криптоанализа;
- квантовая теории информации;
- квантовая механика;
- имитационное моделирование.

Методологическая база квантового криптографического распределения ключей шифрования базируется на разработанных в диссертационном исследовании расширенной классификации квантово-криптографических методов, усовершенствованных моделях квантового детерминистического протокола и методе усиления секретности, а также впервые реализованной комбинированной модели, которые в совокупности обеспечили возможность повышение эффективности безопасного распределения секретных ключей.

Положения, выносимые на защиту

На защиту диссертационной работы выносятся следующие положения:

− разработанные эффективные модели квантового детерминистического протокола в режиме контроля подслушивания и в режиме передачи сообщений,

позволяющие повысить уровень доступности квантового канала и обеспечить безопасное и быстрое распределение ключей;

- предложенный новый метод усиления секретности с использованием квантовых перепутанных состояний пар кутритов и сгенерированных троичных псевдослучайных последовательностей, позволяющий повысить скорость передачи детерминистических протоколов квантовой криптографии без потери стойкости к некогерентной атаке;

− разработанная комбинированная модель на основе разработанных эффективных моделей квантового детерминистического протокола с парами перепутанных кутритов и метода усиления секретности, позволяющая усовершенствовать метод безопасного распределения ключей, обеспечить помехоустойчивость деполяризационного квантового канала.

Практическая значимость научных результатов:

- разработаны модели угроз и нарушителя в квантово-криптографических системах, которые учитывают специфику и уязвимости систем КК, а также возможности нарушителей в соответствии с текущим и перспективным уровнем вычислительных технологий, позволяют определить и выбрать наиболее защищенные методы распределения криптографических ключей. В частности, модель угроз позволяет сформировать концептуальные аспекты предупреждения атак и формализовать возможности превентивных систем в процессе их разработки или усовершенствования. Абстрактная модель нарушителя в системах КК позволяет определить совокупность мероприятий различного характера, которые необходимо дополнительно внедрить для обеспечения надежной защиты применяя специфические квантовые системы;

- в среде MATLAB было разработано соответствующее ПО и проведено имитационное моделирование квантового детерминистического протокола в режимах:

а) контроля подслушивания и, как результат, удалось повысить скорость распределения ключей шифрования минимум в 1, 52 раза при обеспечении защищенности от некогерентной атаки;

б) передачи сообщений, в результате чего получено подтверждение возможности применения предложенной системы помехоустойчивого кодирования над полем Галуа $GF\ (3^2)$ при уровне природных шумов до 10%. Также, это позволит повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом минимум на 3,8%;

- сформулированы практические рекомендации по использованию квантового детерминистического протокола в квантово-криптографических системах в условиях использования деполяризационного квантового канала и присутствия нарушителя;

- программная реализация выполнена на языке программирования C++ в среде разработки Microsoft Visual Studio 2013 (Release версия), а также с использованием специализированных пакетов Wolfram Mathematica 7 и MATLAB R2018a;

- результаты исследования используются в учебном процессе кафедры Кибербезопасность, обработка и хранение информации КазНИТУ имени К.И. Сатпаева (акт внедрения от 02.09.2018), Национального авиационного университета (Киев, Украина) (акт внедрения от 05.09.2018), УО «Белорусская государственная академия связи» (Минск, Беларусь) (акт внедрения от 02.11.2018) и компании AxxonSoft (Киев, Украина) (акт внедрения от 29.10.2018).

Точность и достоверность научных результатов: 1) математическая корректность предложенных моделей и методов; 2) имитационное моделирование режимов работы детерминистического протокола квантовой криптографии; 3) использование лабораторного оборудования для исследования квантово-криптографических протоколов; 4) корректная методика проведения экспериментов в области квантовой криптографии; 5) корректная статистическая обработка полученных экспериментальных данных; 6) соответствие полученных экспериментальных данных теоретическим гипотезам.

Полученные в диссертационной работе результаты могут быть использованы для решения проблемы распределения ключей, а также для повышения эффективности систем криптографической защиты информации.

Публикации и апробация работы

По результатам исследований по теме диссертационной работы было опубликовано 36 работ, из них 6 статей, входящие в базу данных Scopus и Web of Sciences (CEUR Workshops Proceedings (USA), Вестник НАН РК и др.), 3 статьи в журналах, рекомендованных Комитетом по контролю в сфере образования и науки МОН РК, 3 статьи в зарубежных журналах и 21 статья опубликованы в сборниках трудов международных научных конференций в Казахстане и за рубежом.

Основные положения и результаты исследования докладывались и обсуждались на международных форумах, конференциях:

- Международный форум «Инженерное образование и наука в XXI веке: Проблемы и перспективы» (Алматы, 2014);
- Международные Сатпаевские чтения «Роль и место молодых учены в реализации стратегии «Казахстан-2050» (Алматы, 2014);
- II Международная научно-практическая конференция «Информационные и телекоммуникационные технологии: образование, наука, практика» (Алматы, 2015);
- II Международная научно-практическая конференция «Актуальные вопросы обеспечения кибербезопасности и защиты информации» (Украина, Киев, 2016, 2017, 2018);
- Международная научно-практическая конференция «ITSEC: Безопасность информационных технологий» (Украина, Киев, 2016);
- Международная научная конференция УНИТЕХ’16 (Болгария, Габрово, 2016);
- III Международная научно-практическая конференция «Информационная безопасность и компьютерные технологии» (Украина, Кропивницкий, 2018);

- XIV Международная конференция по ИКТ в образовании. «Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer» (Украина, Киев, 2018);

- Международная конференция «Information and Telecommunication Technologies and Radio Electronics - UkrMico» (Украина, Одесса, 2018);

- XVII International Conference on Computer Information Systems and Industrial Management Applications (Россия, Москва, 2018);

- Международная научная конференция «Современные средства связи» (Белоруссия, Минск, 2018);

- VIII Всемирный конгресс «Aviation in the XXI-st century – Safety in Aviation and Space Technologies» (Украина, Киев, 2018);

- VIII Международная научно-техническая конференция «Инфокоммуникации – современность и будущее» (Украина, Одесса, 2018).

- IIV Международная научно-практическая конференция «Актуальні питання забезпечення кібербезпеки та захисту інформації» (Украина, Киев, 2021).

- VII Международная научно-практическая конференция «Актуальні питання забезпечення кібербезпеки та захисту інформації» (Украина, Киев, 2021).

- IV Международная научно-практическая конференция «Department of Information Systems and Technologies. Integration of information systems and intelligent technologies in the conditions of information society transformation» (Украина, Полтава, 2021).

Структура и объем диссертации. Диссертационная работа состоит из введения, четырех разделов, заключения и списка использованных источников и 3 приложений. Работа изложена на 144 страницах машинописного текста, содержит 54 рисунка, 24 таблиц, список использованных источников из 103 наименований.

.

1 АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ БЕЗОПАСНОГО РАСПРЕДЕЛЕНИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

Распределение ключей шифрования является актуальной и важной процедурой, так как криптографический ключ должен быть доставлен к легитимным пользователям своевременно и в условиях полной секретности. На сегодняшний день ключи, как правило, распределяются или средствами асимметричной криптографии, или же с использованием устаревшей и ненадежной схемы доверенного курьера. Безопасность первого метода ставится под угрозу исходя из гипотетических возможностей квантовых компьютеров, а второй метод напрямую связан с человеческим фактором и поэтому априори является ненадежным. Квантовая криптография [6, с. 41, 7, с.4, 9, с.212] в последние годы рассматривается как альтернативный метод и распределения ключей [8, с. 13] и построения современных защищенных систем связи. Именно эти вопросы и будут проанализированы в первом разделе диссертации.

1.1 Проблема распределения ключей в современной криптографии

Проблема распределения секретных ключей является одной из важнейших проблем, связанных с защитой информации, передаваемой по телекоммуникационным каналам. Как только пользователи (субъекты) получают общий секретный ключ, криптограммы можно пересылать по любому незащищенному от прослушивания каналу, возможно даже по каналу, подверженному полному пассивному прослушиванию (например, публичные объявления через средства массовой информации). Однако, чтобы получить общий секретный ключ, два пользователя, у которых изначально нет никакой общей секретной информации, должны использовать какой-то очень надежный и секретный канал. Поскольку перехват представляет собой серию измерений, проведенных подслушивающим агентом, какими бы сложными они не были с технической точки зрения, то любой канал можно в принципе прослушать. Это создает серьезную угрозу безопасности, чем и обусловлена важность обнаружения подслушивающего агента.

Таким образом, секретность передаваемой криптограммы может быть гарантирована только при условии, что ключ (или даже некоторая его часть) не попали к подслушивающему агенту. Следует подчеркнуть, что не существует никакого классического криптографического механизма, гарантирующего, что при передаче по-обычному (не квантовому) коммуникационному каналу ключ не был перехвачен [8, с. 2].

Для решения проблемы безопасного распределения ключей в 1970-х гг. были предложены асимметричные криптосистемы с открытым ключом, которые предлагают математическое решение этой проблемы [1, с. 62, 3, с. 303]. В таких системах пользователям не нужно пересылать секретный ключ перед тем, как послать сообщение. Каждый пользователь имеет пару ключей – открытый и секретный. При этом, зная открытый ключ, в принципе можно раскрыть и секретный. Однако для этого нужно выполнить значительное число математических операций. Например, безопасность системы Ривеста-Шамира-Алдемана (RSA)

основывается на факте простоты перемножения двух больших простых чисел, однако обратная операция – разложение на простые множители полученного произведения – требует значительно больших вычислительных ресурсов [5].

Отметим, что на практике вследствие медленной работы асимметричных криптосистем часто используют гибридную схему [2, с.274]. Пользователи устанавливают общий секретный ключ с помощью схемы Диффи–Хеллмана, или секретный ключ пересылается по схеме цифрового конверта, т.е. отправитель шифрует этот ключ открытым ключом получателя, а получатель расшифровывает его своим секретным асимметричным ключом. Затем этот распределенный общий секретный ключ используется для шифрования потоков данных с помощью алгоритмов симметричной криптографии, например, алгоритмов Data Encryption Standard (DES) или Advanced Encryption Standard (AES), т.к. симметричные криптоалгоритмы выполняются значительно быстрее асимметричных. Отметим, что комбинация RSA + DES или 3DES используется в настоящее время в протоколе SSL, широко применяемый в веб-браузерах и веб-серверах для безопасного обмена приватными данными между пользователями сети Интернет и серверами [1, с. 93, 2, с. 19, 3, с. 266].

Однако, современные асимметричные криптосистемы, как и симметричные, являются «практически надежными». Под *практической надежностью* в криптографии понимают тот факт, что, хотя теоретически такой шифр можно взломать, но практически для этого нужны огромные вычислительные (а соответственно и временные) ресурсы. Возможность взлома 425-битных и даже 512-битных RSA-ключей при помощи объединенных в сеть нескольких сотен современных компьютеров была доказана еще в конце 90-х – начале 2000-х гг. [1, с. 61, 4, с.18]. В настоящее время для корпоративного использования рекомендуются ключи размером минимум 2048 бит, а для шифрования особо конфиденциальной информации – размером 4096 бит. Однако нет никакой гарантии, что и ключи такой длины не будут взломаны, если не при сегодняшнем уровне быстродействия вычислительной техники, то в ближайшем будущем.

Не останавливаясь на детальном анализе преимуществ и недостатков сугубо асимметричных криптосистем, отметим, что в этом случае проблема обнаружения подслушивающего агента снимается, т.к. секретные ключи для симметричного шифрования не распределяются вообще. Но в силу возможности крипто аналитического вскрытия секретного асимметричного ключа, полной секретности такие системы все же не обеспечивают.

Квантовые протоколы распределения секретных ключей [10] предлагают другой подход к решению этой проблемы. Теоретически, квантовая криптография может обеспечить защищенное от перехвата распределение ключа, поскольку, в отличие от классической криптографии, она основана на законах физики, а не на факте того, что для успешного перехвата потребовались бы огромные вычислительные мощности. Вследствие вышеупомянутых свойств квантовых систем, злоумышленник вносит в передаваемую отдельными фотонами информацию некоторое количество ошибок, которые могут быть обнаружены легитимными пользователями. Отметим, что законы квантовой механики [6, с. 32]

позволяют не только обнаружить возмущения состояний, но и связать уровень ошибок при измерениях у легитимных пользователей с количеством информации, которую мог получить злоумышленник. Это позволяет провести процедуру усиления секретности, при которой длина переданного ключа уменьшается на некоторое число бит, зависящее от уровня ошибок при передаче [10, с. 171]. В результате количество информации о ключе, которое может иметь злоумышленник после этой процедуры, ограничено сверху сколь угодно малой величиной, с вероятностью, сколь угодно близкой к единице. Таким образом, протоколы квантового распределения ключей, в отличие от большинства классических схем, имеют теоретико-информационную стойкость, не зависящую от вычислительных и других технических возможностей злоумышленника [6, с. 34].

1.2 Теоретические основы квантовой криптографии

Простейшей квантово-механической системой является квантовый бит (*кубит*) [10, с. 26]. Пространство состояний кубита двумерно. Обозначим базисные векторы в нем, как $|0\rangle$ и $|1\rangle$. Символ $|\ \rangle$ называется *обозначением Дирака*, он обозначает единичный вектор в гильбертовом пространстве. Символ $\langle\ |$ обозначает вектор, эрмитово сопряженный вектору $|\ \rangle$. Произвольный вектор состояния в двумерном гильбертовом пространстве имеет вид:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.1}$$

где α и β – комплексные числа, удовлетворяющие условию $|\alpha|^2 + |\beta|^2 = 1$. Это условие следует из единичности вектора $|\Psi\rangle$: $\langle\Psi|\Psi\rangle = 1$, где символ $\langle\ |\ \rangle$ обозначает скалярное произведение векторов.

Таким образом, кубит является аналогом бита в классической теории информации, который имеет два состояния: «0» и «1». Однако в отличие от бита, кубит может находиться в *суперпозиции* (1.1) двух базисных состояний и тогда невозможно с определенностью утверждать, ни что кубит находится в состоянии $|0\rangle$, ни что он находится в состоянии $|1\rangle$. Однако, согласно постулату измерения в квантовой механике, при измерении кубита будет получено значение «0» с вероятностью $|\alpha|^2$ и значение «1» с вероятностью $|\beta|^2$. Также необходимо подчеркнуть, что (1.1) описывает *когерентную* суперпозицию двух состояний, а не их некогерентную смесь. Для когерентной суперпозиции всегда существует базис, в котором значение кубита строго определено. Так, для состояния $|\Psi'\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ таким базисом является так называемый диагональный базис $\left\{|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right); |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right\}$, повернутый в гильбертовом пространстве

на 45° относительно базиса $\{|0\rangle;|1\rangle\}$. Очевидно, что в таком базисе $|\Psi'\rangle = |+\rangle$ [5, с. 32].

В настоящее время существует множество различных физических реализаций кубитов, используемых для создания квантовых вычислительных устройств [6-7 с., 9-10, с. 237]. Однако в протоколах квантовой криптографии, большинство из которых предназначены для передачи конфиденциальной информации, единственным практичным носителем кубита является фотон, слабо взаимодействующий с другими фотонами и являющийся одним из самых стабильных носителей квантовой информации. В случае, когда носителем кубита является фотон, базисные состояния кубита $|0\rangle$ и $|1\rangle$ соответствуют, например, вертикальной и горизонтальной поляризациям фотона и иногда обозначаются, как $|\beta\rangle$ и $|\leftrightarrow\rangle$ [10, с. 112].

Теорема Холево [11, с. 646]. Предположим, что субъект *A* имеет классический источник информации, который выдает символы $X = 0, \ldots, n$ с распределением вероятностей $p_0, \ldots, p_n$. Субъект *A* готовит квантовое состояние ρ_X, выбирая его из фиксированного набора $p_0, \ldots, p_n$, и посылает это состояние субъекту *Б*, который выполняет квантовое измерение над этим состоянием. Затем он пытается сделать наилучшее предположение о том, как определить *X*, опираясь на результаты своего измерения *Y*. Теорема Холево устанавливает, что для любого такого измерения субъекта *Б* выполняется неравенство

$$H(X:Y) \le S(\rho) - \sum_x p_x S(\rho_x), \tag{1.2}$$

где $H(X:Y)$– взаимная информация между *X* и результатом измерения *Y*; $\rho = \sum_x p_x \rho_x$. Величина в правой части неравенства (1.2) носит название информации (энтропии, величины) Холево, ее обозначают как χ.

Теорема о запрете точного копирования неизвестного квантового состояния [10, с.77]. Эту теорему часто сокращенно называют теоремой о запрете клонирования. Она устанавливает другое ограничение на достижимую квантовую информацию, а именно: невозможность точного копирования неизвестного квантового состояния. Например, классическую информацию в принципе всегда можно скопировать: можно скопировать цифровую информацию – создать копию компьютерного файла. В квантовом случае теорема о запрете клонирования утверждает, что невозможно построить такой квантовый прибор (клонирующую машину), чтобы при наличии на входе состояний $|\psi\rangle$ и $|\varphi\rangle$, на выходе получились две копии входного состояния $|\psi\rangle$, $|\psi\rangle$ или $|\varphi\rangle$, $|\varphi\rangle$. С другой стороны, если состояния $|\psi\rangle$ и $|\varphi\rangle$ ортогональны, то теорема не запрещает их точного копирования. Это разрешает кажущееся противоречие между теоремой о запрете клонирования и возможностью точного копирования классической информации:

классическая информация должна восприниматься, представленной ортогональными состояниями [6, с.420, 7, с. 5, 9, с. 227].

Теорема о запрете клонирования неизвестных квантовых состояний представляет собой один из краеугольных принципов квантовой криптографии. Злоумышленник не может изготовить точную копию квантовых систем, передаваемых по коммуникационному каналу, для проведения измерений над копией, оригинал отправить легитимному пользователю канала, и при этом не измерив его. Это заставляет злоумышленника измерять состояния передаваемых квантовых систем (или перепутывать их со своими вспомогательными системами), что вследствие постулата измерения приводит к изменению их состояний. Такие изменения передаваемых состояний могут выявить легитимные пользователи канала, выполнив квантовые измерения и обменявшись результатами этих измерений по обычному открытому каналу связи. Отметим, что вероятность правильного копирования произвольного состояния кубита, создание одной его копии, равняется 5/6. Если нужно создать *n* копий неизвестного состояния кубита, то вероятность правильного копирования уменьшается и при $n \to \infty$ стремится к 2/3 [11, с. 647].

Неразличимость не ортогональных квантовых состояний. Вследствие изложенных выше постулатов квантовой механики, невозможно выполнить измерение, которое позволило бы точно различить два состояния кубита $|\Psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ и $|\Psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$, кроме случая, когда эти состояния ортогональны $(\langle\Psi_1|\Psi_2\rangle = 0)$. Это утверждение справедливо не только для кубитов, но и для квантовых систем любой размерности [10, с. 58].

Теоретико-информационная стойкость квантовых протоколов распределения ключей требует оценки количества информации, которая могла бы попасть к злоумышленнику при реализации протокола. Утечка информации к злоумышленнику происходит при выполнении первых двух элементов стека. Полный учет всех факторов, которые влияют на утечку, является крайне сложной задачей. Эта задача в настоящее время частично решена только для нескольких наиболее простых протоколов, например, протокола BB84 [9, с.213]. Поэтому, в качестве приближенной оценки, как правило, рассматривают только информацию, которая попадает к злоумышленнику (субъект *E*) при выполнении протокола квантовой передачи. Соответствующая количественная характеристика – это наибольшая из двух величин: взаимная информация Шеннона $I_{AE}(D)$ между субъектами *A* и *E* или $I_{BE}(D)$ между субъектами *Б* и *E*. Эти величины являются функциями уровня ошибок *D*, вносимых атакой. Отметим, что наибольшая из этих величин является только нижней границей утечки информации, но дополнительный анализ утечки при исправлении ошибок для протокола BB84 увеличивает эту границу не более, чем на несколько процентов. Таким образом, функции $I_{AE}(D)$ или $I_{BE}(D)$ можно считать приемлемой характеристикой стойкости любого квантового протокола распределения ключей [6, с. 37].

Перепутывание (квантовая корреляция). Две или более квантовых системы могут быть коррелированы или перепутаны. Так, пара фотонов в синглетном поляризационном состоянии:

$$\left\{\left|\Psi_{ij}\right\rangle\left\langle\Psi_{ij}\right|\right\}, \tag{1.3}$$

является примером максимально перепутанного состояния. Состояние (1.3) называют парой Эйнштейна-Подольского-Розена (ЭПР-парой).

Если измерение выполняется в вычислительном базисе над одним из двух перепутанных кубитов в состоянии (1.3), то результат будет случайным: «0» или «1» с равной вероятностью 1/2. Состояние второго кубита *антикоррелировано* с состоянием первого, т.е. если первый кубит в результате измерения переходит в состояние «0», то второй перейдет в состояние «1», и наоборот. Без проведения измерения, однако, ни один из этих кубитов не находится в определенном состоянии (состояние каждого из этих кубитов по отдельности является смешанным). Отметим, что квантовое перепутывание, как и суперпозиция квантовых состояний – это исключительно квантовые эффекты, не имеющие аналога для объектов классической физики.

Четыре максимально перепутанных ортогональных состояний в системе двух кубитов образуют базис Белла:

$$\left|\Phi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right);\qquad \left|\Phi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right);$$
$$\left|\Psi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right);\qquad \left|\Psi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle-\left|10\right\rangle\right). \tag{1.4}$$

Одним из простых перепутанных состояний трех кубитов является состояние Гринбергера-Хорна-Цайлингера (ГХЦ):

$$\left|GHZ\right\rangle=\frac{1}{\sqrt{2}}\left(\left|000\right\rangle+\left|111\right\rangle\right). \tag{1.5}$$

Как и для двухкубитных состояний Белла (1.4), в ГХЦ-состоянии (1.5) каждый из трех кубитов находится в полностью смешанном состоянии и не несет сам по себе никакой информации. Однако, если измерить состояние одного из кубитов в состоянии (1.5), то два других сразу принимают определенные значения. Таким образом, измерение разрушает перепутанность состояний вида (1.4) – (1.5) [11, с. 38].

1.3 Анализ современных методов распределения ключей на базе протоколов квантовой криптографии

Большинство предложенных к настоящему времени протоколов КК (см. рисунок 1.1 [12, с. 80]) используют двухуровневые квантовые системы – *кубиты),* что позволяет передавать классическую информацию битами.

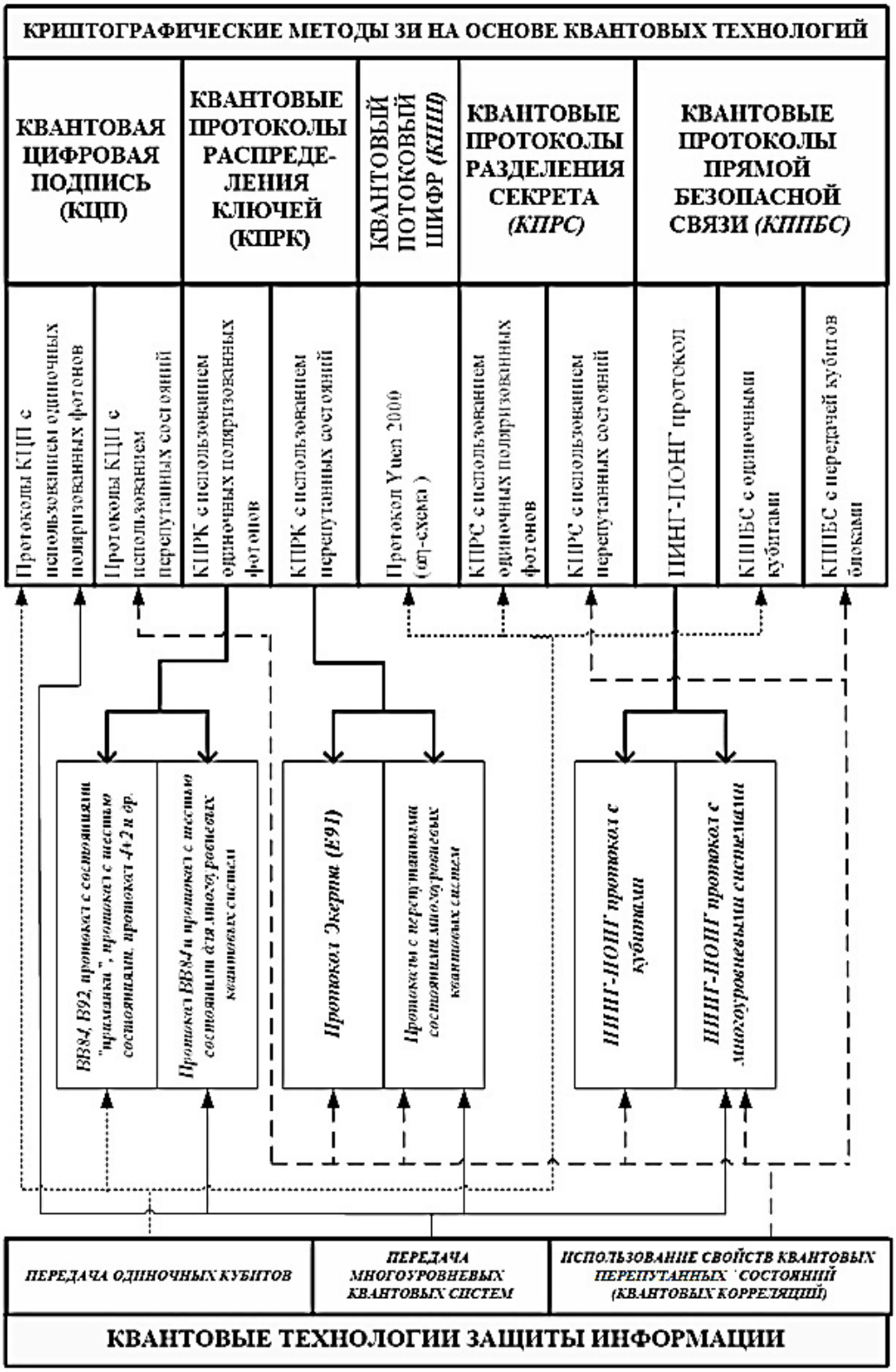


Рисунок 1.1 – Классификация квантовых методов защиты информации

Однако информационную емкость квантовых протоколов можно повысить, используя многоуровневые квантовые системы, т.е. передавая классическую информацию тритами, квартами т.д. – соответственно трехуровневая квантовая система получила название *кутрит,* четырехуровневая – *кукварт* и т.д.

В общем случае *d*-уровневая квантовая система называется кудитом (qudit). С технической точки зрения в протоколах квантовой криптографии носителями как кубитов, так и многоуровневых квантовых систем являются фотоны, но оперировать с многоуровневыми системами несколько сложнее, чем с кубитами. Таким образом, протоколы квантовой криптографии можно разделить на две большие группы относительно того, двух- или многоуровневые квантовые системы в них используются. С другой стороны, квантовые системы, состоящие из двух или более квантовых частиц, могут находиться в перепутанных состояниях, т.е. в таких состояниях между этими частицами существуют исключительно квантовые корреляции. Локальные операции над одной из частиц перепутанного состояния приводят к изменению всего состояния, что позволяет кодировать классическую информацию, действуя на одну из частиц, в то время как вторая находится у другого абонента квантового протокола. Использование свойств квантовых перепутанных состояний позволяет обеспечить высокий уровень безопасности протоколов квантовой криптографии, а также повысить их эффективность. Таким образом, протоколы квантовой криптографии можно разделить на две большие группы относительно того, одиночные или перепутанные квантовые системы в них используются.

Современные протоколы квантовой криптографии. Обеспечение теоретико-информационной устойчивости (безусловная устойчивость, которая не зависит от вычислительных возможностей злоумышленников) является главным преимуществом *квантового распределения ключей.* Этот метод включает в себя следующие протоколы [12, с. 78]:

- протоколы с использованием одиночных поляризованных фотонов;
- протоколы с использованием фазового кодирования;
- протоколы с использованием перепутанных состояний;
- протоколы с состояниями «приманки».

Идея использования квантовых объектов для ЗИ была впервые предложена в 1970 году Стефаном Виснером. В 1984 году Чарльз Беннет из компании IBM и Жиль Брассар из Монреальского университета развили идею Стефана Вейснера и предложили первый протокол [9, с.45] квантовой криптографии (см. рисунок 1.2), который должен был стать альтернативным и нетрадиционным решением проблемы распределения ключей шифрования. Этот протокол получил название *BB84*, он относится к квантовым протоколам КРК с использованием *одиночных поляризованных фотонов*. Основными задачами КРК является генерация и распределение ключей шифрования между двумя абонентами, которые соединены квантовым и классическим каналами связи [7, с.38]. В большинстве протоколов с единичными поляризованными фотонами используются 4 поляризованные состояния фотонов (0º, 45º, 90º, 135º), которые передаются квантовым каналом связи. Поиск и исправления ошибок выполняются с использованием открытого

классического канала, который не должен быть конфиденциальным, а только аутентифицированным. Для обнаружения факта действия злоумышленника используется процедура контроля ошибок, а для обеспечения безусловной устойчивости используется классическая *процедура усиления секретности (privacy amplification)* [9, с. 224, 11, с.706].

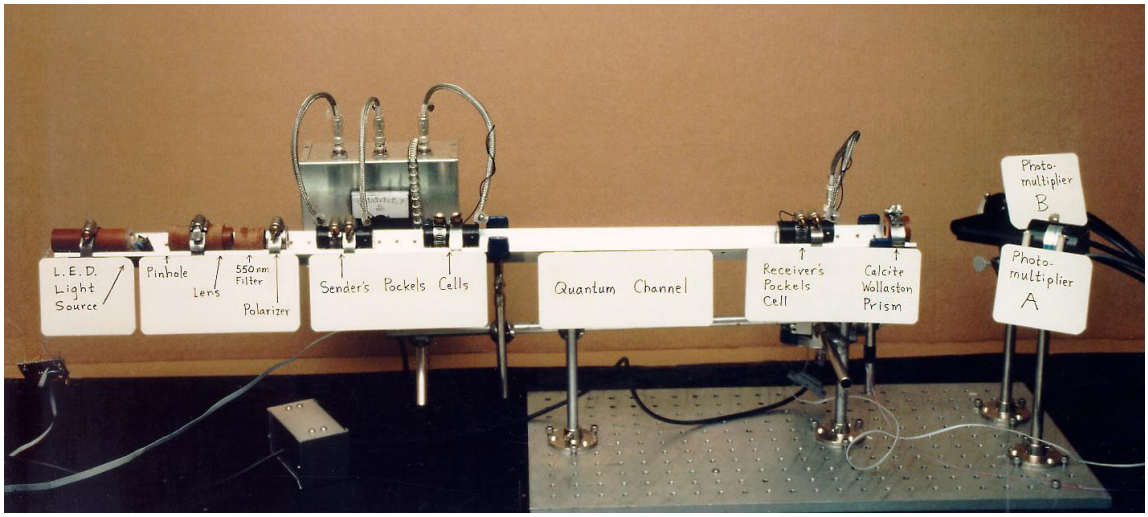


Рисунок 1.2 – Первая экспериментальная установка КРК BB84

Эффективность протокола BB84 с кубитами в идеальных условиях равна 50%. Под *эффективностью* (именно в квантовой криптографии и КРК) будем понимать отношение количества фотонов, которые используются для генерации ключа, к общему количеству переданных фотонов. Кроме этого, в работе [13, с.27] предложено обобщение протокола BB84 на многоуровневые квантовые системы (*протокол BB84 с кудитами*). Этот протокол имеет значительно большую информационную ёмкость и устойчивость к некогерентным атакам, но его сложнее реализовать с технической точки зрения.

Исходными данными КРК является ключевая последовательность, которая может быть использована для дальнейшего шифрования данных. К вышеупомянутому типу протоколов КРК кроме BB84 также относятся:

- протокол с шестью состояниями;
- протокол 4+2;
- протокол Гольденберга-Вайдмана;
- протокол Коаши-Имото.

Протокол с шестью состояниями [12, с. 80] предусматривает использование четырех состояний, аналогичных протоколу BB84 и дополнительно вводятся еще два возможных направления поляризации – право циркулярный и лево циркулярный. Такие изменения с одной стороны уменьшают количество информации, которая может быть получена злоумышленником, а с другой стороны эффективность протокола также уменьшается (до 33%). Также предложено обобщение протокола с шестью состояниями на многоуровневые квантовые системы. Данный протокол имеет несколько большую информационную ёмкость и значи-

тельно большую устойчивость к атаке «перехвата - повторной посылки» кудитов. Устойчивость протокола к общей некогерентной атаке практически такая же, как и у протокола BB84 с кудитами.

Протокол 4+2 [12, с. 81] является переходным между BB84 и B92. В нем используются 4 квантовые состояния для кодирования «0» и «1» в двух базисах. Состояния в каждом базисе выбираются не ортогональными, кроме того, состояния в разных базисах также должны быть попарно не ортогональными. Для протокола 4+2 характерно меньшее количество ошибок относительно протокола BB84 для кубитов и меньшее количество полезной информации, которую может получить злоумышленник, но одновременно происходит и уменьшение относительной эффективности данного протокола.

В *протоколе Гольденберга-Вайдмана* [12, с. 81] кодирование «0» и «1» выполняется с помощью двух ортогональных состояний. Каждое из этих состояний является суперпозицией двух локализованных нормализованных волновых пакетов. Для защиты против атаки «перехвата – повторной посылки» используется случайное время отправления пакетов.

Модифицированный вариант протокола Гольденберга-Вайдмана – это *протокол Коаши-Имото* [12, с.82], усовершенствованный тем, что вместо случайного времени отправления пакетов используется ассиметризация интерферометра, то есть свет разбивается в неравных пропорциях между длинным и коротким плечами интерферометра.

Следующий тип КРК – протоколы квантового распределения ключей с *использованием фазового кодирования* [12, с.82]. Самым известным представителем данного типа протоколов является *B92* – концептуально самый простой квантовый протокол, в котором используются любые два не ортогональные поляризованные состояния фотонов, а выявление факта атаки злоумышленника происходит аналогично процедурам, описанным выше для протокола BB84. Эффективность данного протокола составляет 25%, поэтому он не является практически важным протоколом.

*Протокол Экерта (*он же *E91)* [12, с. 82], относится к КРК с и*спользованием перепутанных состояний.* Во время передачи информации по протоколу E91, перехват одного из фотонов пары не дает злоумышленнику никакой полезной информации. Кроме того, предложено обобщение схемы Экерта на трехмерные, и многомерные квантовые системы, что значительно увеличивает информационную ёмкость протокола.

Протокол SARG04 [12, с.83] имеет небольшие отличия от оригинального протокола BB84, которые не касаются его «квантовой» части (то есть здесь он совпадает с протоколом BB84), а касаются только «классической» процедуры просеивания ключа, которая выполняется в этих протоколах после квантовой передачи. Такое усовершенствование позволяет повысить устойчивость протокола к *атаке разделения количества фотонов* (*photon number splitting attack*) [12, с.81]. Также при реализации протоколов на реальном оборудовании SARG04 имеет более высокую скорость генерации ключа и может выполняться для больших расстояний между легитимными абонентами, чем протокол BB84.

Протоколы с состояниями «приманки» (decoy states protocols) является усовершенствованным вариантом протокола BB84, в котором отправитель, путем замены подмножества импульсов, вводит так называемые приманки [12, с.83]. Как показывают практические эксперименты [12, с.84], данному типу протоколов характерен более высокий уровень безопасности, чем в BB84. Кроме того, такие протоколы отличаются устойчивостью против атаки разделения количества фотонов. К явным преимуществам протоколов с состояниями «приманки» также можно отнести и увеличение длины канала за счет линейной зависимости от потерь в канале. Однако, без предварительной аутентификации пользователей на таких протоколах невозможно решить проблему распределения криптографических ключей.

Результаты многокритериального анализа современных квантово-криптографических протоколов распределения ключей приведены в таблице 1.1 по следующим критериям:

IC – возможность увеличения информационной емкости;

SA – защищенность (устойчивость) от известных атак;

MU – возможность передачи ключа более чем одному пользователю;

ID – возможность обнаружения злоумышленника;

TI – возможность обеспечения теоретико-информационной стойкости;

EF – эффективность (0 – 100%).

Таблица 1.1 - Сравнение эффективности протоколов КК

Протоколы КК	*IC*	*SA*	*MU*	*ID*	*TI*	*EF*
BB84	+/-	+/-	-	+/-	+	≤50%
Six States	+	+/-	-	+/-	+	≤33%
4+2	-	-	-	+/-	-	≈25%
Goldenberg-Vaidman	-	-	-	+/-	-	≤30%
Koashi-Imoto	-	+/-	-	+/-	-	≤30%
B92	-	+/-	-	+/-	+	25%
E91	+	-	+	+	+/-	>50%
SARG04	-	+	-	+/-	+	≤50%
Deterministic	+	+/-	+	+	+/-	>50%
Decoy States	-	+	-	+/-	+	≤50%
COW	-	+/-	-	+/-	+/-	≤50%
DPS	-	+/-	-	-	+/-	≤50%

Исходя из результатов проведенного анализа, можно отметить, что детерминистический протокол является достаточно эффективным (>50%), имеет возможность увеличения информационной емкости (за счет использования кудитов), а также имеет возможность передачи ключа более чем одному пользователю (за счет использования троек/четверок и т.д. кубитов (кудитов) вместо пар). Поэтому этот протокол будет использоваться в диссертационной работе как ба-

зовый. Несмотря на преимущества, детерминистический протокол имеет несколько недостатков, которые требуют разработки и внедрения дополнительных процедур, например, для обеспечения теоретико-информационной стойкости (т.к. базовый детерминистический протокол имеет только асимптотическую стойкость).

1.4 Обзор коммерческих квантовых систем распределения ключей

В настоящее время реализовано значительное количество экспериментов на лабораторном оборудовании по КРК, например, [14, с.39, 20-23]. Существуют также уже готовые системы, полностью пригодные для интеграции в современные телекоммуникационные сети. Первой такой системой была QPN Security Gateway (QPN-8505) (см. рисунок 1.3), созданная компанией MagiQ Technologies (США). Данная система предлагает защиту VPN с помощью квантового распределения ключей (до ста 256-битных ключей в секунду на расстояние до 140 км) и интегрированного шифрования. Система QPN-8505 для квантового распределения ключей использует протокол BB84 с фазовым кодированием.

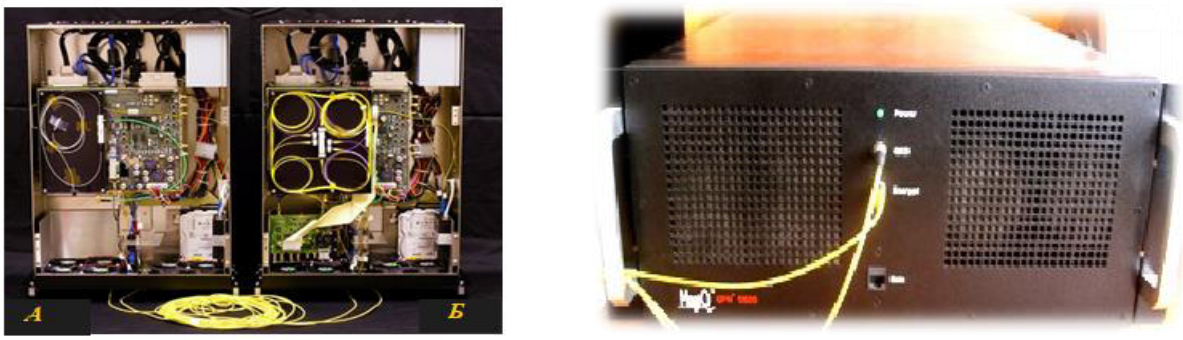


Рисунок 1.3 – Система QPN-8505

Швейцарская компания Id Quantique (см. рисунок 1.4) предлагает систему под названием Cerberis [21], которая представляет собой сервер с автоматическим созданием и секретным обменом ключами через оптоволоконный канал. Данная система может передавать криптографические ключи на расстояние до 50 км, ее характерной особенностью является 12 параллельных криптографических вычислений, что значительно повышает быстродействие. Система Cerberis использует для шифрования симметричный протокол AES с ключом длиной 256 бит, а для квантового распределения ключей – протоколы BB84 и SARG.

Id Quantique также предлагает масштабную линейку генераторов ПСЧП и комплектующих для лабораторных систем (см. рисунок 1.5) [23].

Система КРК Cerberis QKD

> Доказуемый безопасный обмен ключами на основе КРК
> Квантовые ключи обеспечивают долгосрочную защиту
> Полностью автоматизированный обмен ключами с непрерывным их обновлением
> Интегрированный источник энтропии на основе квантового генератора случайных чисел

Платформа КРК QKD Clavis³

> Открытая платформа КРК для приложений
> Высокоскоростная генерация и распределения ключей до 100 км
> Односторонний когерентный протокол (ОКП) (патент по IDQ)
> Устройство на основе протокола передачи ключа

Рисунок 1.4 – Квантовые системы от Id Quantique

Рисунок 1.5 – Комплектующие от Id Quantique

Также недавно компанией Toshiba Research Europe Ltd (Великобритания) была представлена еще одна система квантового распределения ключей под названием Quantum Key Server (см. рисунок 1.7) [22]. Эта система обеспечивает генерацию до ста 256-битных ключей в секунду и их одностороннюю передачу от передатчика к приемнику. В ее состав входит интегрированный модуль автоматического управления, который проводит непрерывный мониторинг системы Quantum Key Server и регулирует оптические характеристики.

Рисунок 1.6 – Система Quantum Key Server

Рисунок 1.7 – Применение системы Quantum Key Server

Еще одна британская компания QinetiQ представила первую в мире сеть, использующая квантовую криптографию – Quantum Net (Qnet) [14, с.40]. Максимальная длина линий связи данной сети составляет 120 км, а самое главное, что система Qnet – это первая квантово-криптографическая система, использующая более 2 серверов. Их в данной системе 6 и все они являются интегрированными в сеть Internet.

Стоит также отметить компанию Labs Quintessence (см. рисунок 1.8).

Рисунок 1.8 – Система qCrypt от Labs Quintessence

Также, невозможно не выделить т.н. «китайский квантовый прорыв» (см. рисунок 1.9), в частности квантовые спутниковые технологии:

Рисунок 1.9 – Китайский квантовый спутник MICIUS

Анализ существующих методов, коммерческих систем, а также реализованных к настоящему времени теоретических и экспериментальных работ в области КРК позволяет выделить следующие их достоинства и недостатки [14, с.40].

К *достоинствам* можно отнести:

1. Протоколы квантового распределения ключей позволяют всегда обнаружить атаку пассивного перехвата, т.к. подключение злоумышленника вносит в квантовый канал значительно большой уровень ошибок по сравнению с уровнем естественных помех в канале.

2. Безусловная (теоретико-информационная) безопасность квантовых протоколов распределения ключей позволяет использовать совершенно секретный ключ для дальнейшего шифрования известными классическими симметричными алгоритмами – это соответственно увеличивает уровень защищенности, который обеспечивают чисто классические криптосистемы. Также возможен синтез квантовых протоколов распределения ключей с шифром Вернама (одноразовым блокнотом), что в сочетании с безусловно стойкой схемой аутентификации даст абсолютно стойкую систему обмена сообщениями.

К *недостаткам* протоколов КРК относятся:

1. Система, построенная только на квантовых протоколах распределения ключей, не может служить полноценным завершенным решением проблемы распределения секретных ключей – нужны также средства для предварительной аутентификации пользователей. Такая аутентификация может быть выполнена, например, с помощью начального небольшого секретного ключа, который пользователи системы квантового распределения ключей должны получить один раз заранее. Затем небольшую часть секретного ключа, распределенного с помощью квантового протокола, пользователи могут оставить для аутентификации в следующем сеансе и т.д.

2. Ограничение длины квантового канала: при передаче квантовой информации невозможно «усилить сигнал» из-за невозможности клонирования квантовых состояний. Однако можно создать квантовый аналог повторителя, что дает возможность передачи квантовой информации на большие расстояния посредством создания перепутанных состояний между отправителем и получателем. Это перепутывание потом может быть использовано при квантовой коммуникации, в частности, в квантовых протоколах распределения ключей. Технология квантовых повторителей, основанная на технологии квантовой памяти, активно разрабатывается в настоящее время, но эта технология пока еще не вышла за пределы лабораторных экспериментов.

3. Низкая эффективность (вероятность зарегистрировать отсчет, если фотон попал в детектор) детекторов одиночных фотонов – для телекоммуникационного «окна прозрачности» 1550 нм эффективность таких детекторов, работающих при температурах 200-300 К, не превышает 10%. Существуют также сверхпроводящие детекторы, работающие при сверхнизких температурах 0, 1-1, 5 К, эффективность которых достигает 95%. Однако использование таких сверхпроводящих детекторов в квантовых системах распределения ключей значительно увеличивает стоимость системы. Еще одна проблема, связанная с детекторами – эффект «темнового шума», когда детектор срабатывает при отсутствии фотона.

4. Скорость передачи информации по квантовому каналу существенно уменьшается с увеличением длины канала и в большинстве экспериментов на расстояниях порядка 100 км равна нескольким битам в секунду (в недавней работе – на расстоянии в 100 км достигнута скорость 10, 1 кбит/с, а при использовании сверхпроводящих детекторов одиночных фотонов – 17 кбит/с на расстоянии 105 км и 12, 1 бит/с на расстоянии 200 км).

5. Деполяризация фотонов в квантовом канале, которая приводит к ошибкам при измерениях у легитимных пользователей.

6. Сложность технической реализации протоколов с многоуровневыми квантовыми системами.

7. Высокая цена предлагаемых сегодня на рынке готовых систем квантового распределения ключей.

Таким образом, в первом разделе диссертационной работы проведен анализ современных методов, моделей и коммерческих систем распределения ключей шифрования по критериям безопасности (защищенности) и скорости. В результате этого была получена классификация квантово-криптографических методов (п.2.1), которая за счет расширения множества известных базовых признаков, частичных обобщений теоретических положений и практических достижений в области квантовой криптографии, позволяет расширить возможности по выбору необходимых квантово-криптографических методов для построения безопасных систем распределения ключей шифрования.

С точки зрения эффективности и скорости работы, наиболее подходящим для внедрения, является детерминистический протокол квантовой криптографии, хотя с точки зрения безопасности есть много аспектов, которые нужно проработать. Например, по сравнению с КРК, детерминистические протоколы КПБС

обладают лишь асимптотической стойкостью, что позволяет злоумышленнику перехватить некоторое количество информации (некогерентная атака), поэтому нужно разрабатывать дополнительные процедуры предварительной и постобработки – этот аспект будет непременно учитываться в последующих разделах диссертационной работы.

2 МОДЕЛИ УГРОЗ И НАРУШИТЕЛЯ В СИСТЕМАХ КВАНТОВОЙ КРИПТОГРАФИИ

Исходя из результатов первого раздела диссертации, одним из наиболее эффективных методов решения проблемы распределения ключей, является использование КРК. Стоит также отметить, что сегодня среди существующих квантовых технологий именно КРК, не смотря на ряд недостатков, реализовано практически (в виде отдельных модулей (раздел 1.4) либо же подсистем, которые интегрируются в существующие информационно-коммуникационные системы) и вышло за грани лабораторных экспериментов. Кроме этого, системы КРК являются объектом атаки и требуют от нарушителя новых знаний и умений. В этой связи, второй раздел диссертации посвящен моделям угроз и нарушителя в системах КРК.

2.1 Разработка расширенной классификации квантово-криптографических методов распределения ключей шифрования

Согласно современным исследованиям [7-15], а также базируясь на результатах, полученных в первом разделе диссертационной работы, протоколы КРК могут быть разделены на классы:

- протоколы с использованием одиночных кубитов (протоколы типа «приготовление – измерение»);
- протоколы с использованием одиночных многоуровневых квантовых систем (кудитов);
- протоколы с использованием перепутанных состояний кубитов;
- протоколы с использованием перепутанных состояний кудитов.

В результате исследования существующих методов квантовой криптографии, разработана расширенная классификация методов КРК (см. рисунок 2.1) [24-25]. В этой классификации также отмечены конкретные квантовые атаки, к которым уязвимы протоколы, которые анализировались в первом разделе диссертации. Эти атаки будут детально рассматриваться в следующем подразделе работы (пп. 2.2), посвященный разработке модели угроз в системах КК – без подобной модели невозможно построить эффективную систему информационной безопасность, в том числе, которая базируется на квантовых технологиях.

Таким образом, расширена классификация квантово-криптографических методов распределения ключей шифрования, которая за счет расширения множества известных базовых признаков, частичных обобщений теоретических положений и практических достижений в области квантовой криптографии, позволяет расширить возможности относительно выбора необходимых квантово-криптографических методов для построения стойких систем распределения ключей шифрования [24-28].

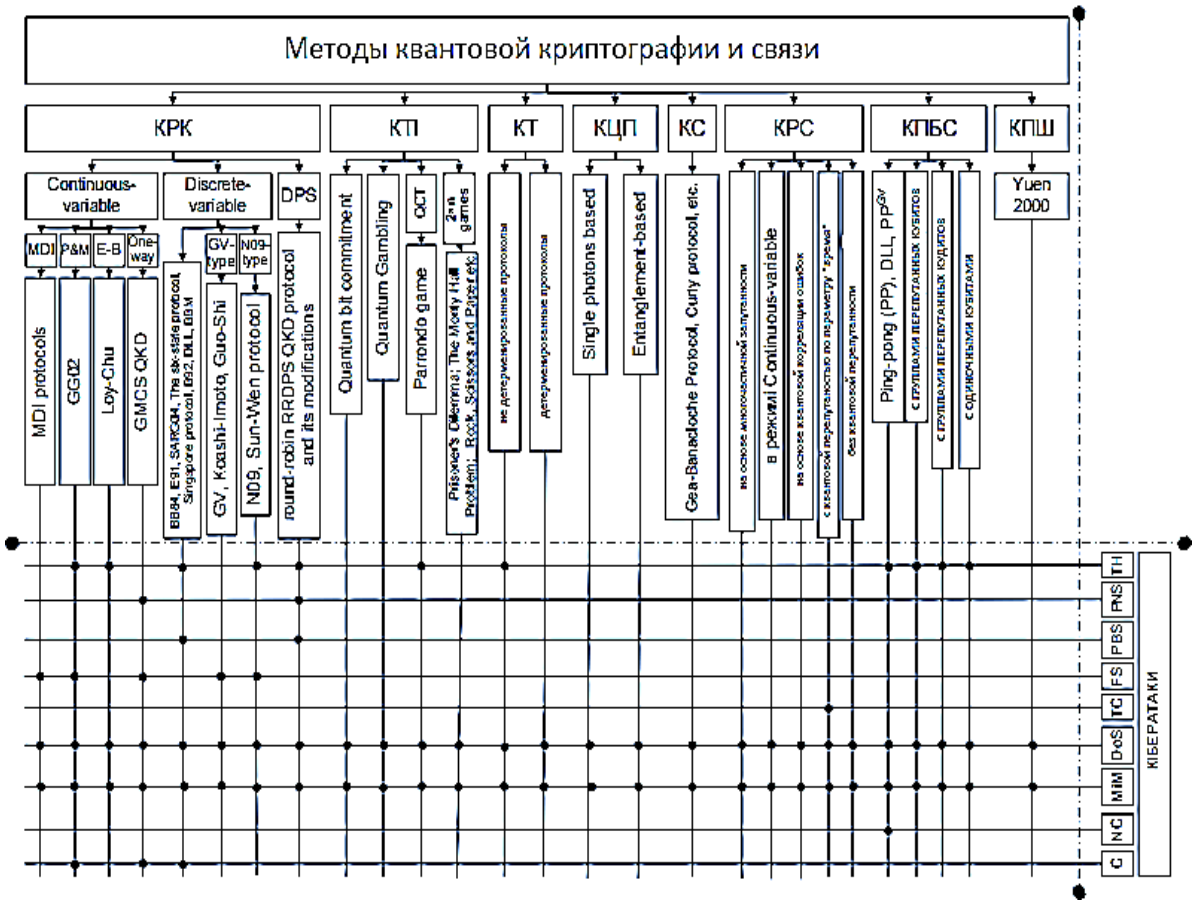


Рисунок 2.1 – Расширенная классификация протоколов КРК [24, с.290]

2.2 Модель угроз в системах квантовой криптографии

Наиболее простым способом съема информации в обычных оптических телекоммуникационных сетях является разделение пучка фотонов. Однако в протоколах квантовой криптографии передача должна происходить при помощи одиночных фотонов, и в таком случае нарушитель не сможет отвести часть сигнала. Поэтому, подобные МПИ не могут быть применены в квантовых системах в идеальных условиях однофотонных сигналов (к тому же, такие источники пока не созданы). На практике сейчас используют слабые когерентные импульсы, излучаемые лазерными светодиодами. Число фотонов в импульсе определяется распределением Пуассона, то есть часть передаваемых импульсов содержит два и более фотона. Вероятность зарегистрировать в импульсе более одного фотона при передаче их каналом с потерями определяется по формуле (2.1) [15, с.114]:

$$p_{n>1} = 1 - e^{-\eta\mu}\left(1+\eta\mu\right), \tag{2.1}$$

где μ – среднее число фотонов в импульсе, η – коэффициент передачи канала.

Таким образом, МПИ с разделением пучка фотонов на текущий момент возможны и в квантовой криптографии. На рисунке 2.2 показана предложенная обобщенная классификация МПИ в ИКС на основе КТ:

Рисунок 2.2 – Обобщенная классификация МПИ в ИКС на базе КТ

Рассмотрим сначала МПИ [15-16, с. 110, 22, 29-34], которые могут быть использованы злоумышленником при условии, что легитимные пользователи реализуют квантовый протокол с идеальными однофотонными источниками сигналов. В этом случае МПИ по степени сложности можно разделить на *когерентные* и *некогерентные*. При некогерентных МПИ злоумышленник обрабатывает каждый фотон, который передается по квантовому каналу, отдельно. В свою очередь, некогерентные МПИ бывают *непрозрачными* и *полупрозрачными*. Непрозрачные МПИ [15, с.111] состоят в измерении злоумышленником непосредственно квантового состояния фотона и дальнейшей повторной отправке нового фотона в состоянии, полученном в результате измерения. Поскольку злоумышленник не пропускает квантовые состояния отправителя, а генерирует новые и отправляет их принимающей стороне, то данный класс МПИ называется непрозрачным.

Полупрозрачные МПИ [15, с.112] предусматривают использование злоумышленником вспомогательных квантовых систем (квантовых проб) для перепутывания их с носителями, которые субъект А (отправитель) пересылает субъекту Б (получателю) по квантовому каналу. После перепутывания, передаваемые и вспомогательные состояния находятся в общем перепутанном состоянии, затем первые передаются субъекту Б, а другие сохраняются в квантовой памяти злоумышленника. После окончания открытого обмена информацией между субъектами А и Б на этапе просеивания ключа, в частности объявления базисов, в которых субъект Б измерял фотоны, злоумышленник определяет последовательность базисов, которую необходимо использовать для измерения состояний его проб, чтобы получить как можно больше информации о ключе. Состояния фотонов, посылаемые субъектом А, меняются после перепутывания с пробами злоумышленника, однако уровень ошибок при данной атаке значительно ниже, чем при непрозрачной. Следует отметить, что для реализации подобного МПИ злоумышленнику необходимо иметь квантовую память большого объема для хранения проб до объявления базисов субъектом Б, а также сложное оборудование для перепутывания своих проб с фотонами субъекта А. Полупрозрачные

МПИ являются также одним из основных видов съема информации в протоколах квантовой прямой безопасной связи. В [15, с.126] проанализирована атака с использованием квантовых проб на детерминистический протокол КПБС с ГХЦ-триплетами, а также вычислена полная вероятность обнаружения атаки злоумышленника в зависимости от количества полученной им информации для трех различных вариантов пинг-понг протокола. Аналогичный анализ атаки на пинг-понг протокол с перепутанными парами кутритов (квантовых тритов, т.е. квантовых троичных систем) выполнен в [12, с.82], где также доказано, что информационная емкость и стойкость различных вариантов этого протокола являются обратно пропорциональными величинами.

При *когерентных МПИ* [15, с.113] злоумышленник может любым (унитарным) способом перепутать пробу любого размера с группой передаваемых фотонов. Одним из подвидов данного класса МПИ является *коллективная атака*. Данная атака похожа на полупрозрачную в начальной стадии, то есть каждый фотон, посылаемый субъектом А, индивидуально перепутывается с отдельной пробой. Итак, злоумышленник получает пробы в таких же состояниях, как и при полупрозрачной атаке. Но после окончания открытого обмена информацией между легитимными пользователями, злоумышленник выполняет так называемое обобщенное измерение сразу на всех квантовых пробах как на единственной квантовой системе. Объединённая атака это наиболее эффективный МПИ в квантовых системах. Представляет собой частный случай когерентных МПИ, когда злоумышленник использует единую квантовую пробу (из гильбертова пространства [11, с. 81] состояний большей размерности) для перепутывания со всей последовательностью фотонов, которые субъект А передает субъекту Б. Но этот МПИ является и наиболее сложным с технической точки зрения. Подводя итоги, следует отметить, что в соответствии с современным уровнем технологий квантовой информатики*, реализация когерентных МПИ невозможна* (в отличие от некогерентных) [11, с.114], так как еще не существует необходимых для этого квантовой памяти большого объема и многокубитного квантового компьютера (хотя относительно последнего стоит отметить, что, в принципе, такой компьютер уже существует, но его вычислительные возможности еще не подтверждены экспериментально).

Методы перехвата информации, обусловленные несовершенством протоколов. Несовершенство квантовых протоколов является серьезным фактором для реализации разнообразных МПИ и других атак в ИКС на основе КТ. Известным МПИ этого класса является атака «человек посередине» (man-in-the-middle attack). Для реализации этой атаки злоумышленник должен полностью контролировать классический (не квантовый) канал связи между легитимными пользователями, а именно иметь возможность заменять все сообщения, передаваемые этим каналом связи. Таким образом, злоумышленник имеет возможность полностью снять информацию, которой обмениваются легитимные пользователи в квантовом канале (например, узнать все биты ключа), и при этом не быть обнаруженным легитимными пользователями. Следует отметить, что все существу-

ющие протоколы КРК и квантовой прямой безопасной связи уязвимы относительно этой атаки. *Защита от такой атаки* является общеизвестной – это аутентификация сообщений легитимных пользователей в классическом канале.

Атака «отказ в обслуживании» (denial of service attack) не относится к МПИ, это метод нарушения связи между легитимными пользователями. Для оригинального пинг-понг протокола [9, с.218] такого рода атака была рассмотрена в [32, с.19]. Суть ее состоит в том, что злоумышленник не перепутывает свою квантовую пробу с кубитом на пути от субъекта Б к субъекту А, а просто измеряет состояние кубита на обратном пути от субъекта А к субъекту Б (т.е. после кодирования информации субъектом А) – тем самым нарушая взаимную корреляцию кубитов у субъектов А и Б. В результате злоумышленник не получит никакой полезной информации, но разрушит квантовый канал (нарушит его секретность) между легитимными пользователями. В случае протокола с ГХЦ-триплетами злоумышленник может также измерять состояния одного или двух кубитов и нарушать, таким образом, перепутанность состояния триплета [6, с.249]. Отметим, что к атаке «отказ в обслуживании» также уязвимы практически все протоколы квантовой криптографии.

Методы перехвата информации, обусловленные несовершенством оборудования. В классической криптографии МПИ, обусловленные несовершенством оборудования, называют также *МПИ, которые используют утечку информации по побочным каналам*. Как можно было предположить, МПИ такого вида также возможны и в квантовой криптографии.

Атаки типа «Троянский конь». К таким атакам уязвимы так называемые двухсторонние (two-way) протоколы КРК и квантовой прямой безопасной связи, а именно протоколы, в которых фотоны пересылаются от субъекта Б к субъекту А и обратно. Примером такого протокола является вышеупомянутый пинг-понг протокол. Злоумышленник посылает световые импульсы в квантовый канал, соединяющий аппаратуру легитимных пользователей, а затем анализирует отраженный свет. Таким способом в принципе можно выявить, какой лазер или какой датчик только что сработал, или параметры настройки модуляторов поляризации и фазы. Такая атака не может быть просто предотвращена использованием задвижки, потому что легитимные пользователи должны оставить «двери открытыми» для своих фотонов. Но они могли бы обнаружить дополнительные фотоны злоумышленника, так как при такой атаке происходит увеличение энергии импульсов. Поэтому злоумышленник должен использовать свет другой длины волны, чем тот, который используют легитимные пользователи, а именно такой длины, к которой их датчики нечувствительны [15, с.113]. Другой способ для злоумышленника скрыть атаку заключается в том, что он перехватывает сигнал, который передается от субъекта Б к субъекту А, и затем вставляет дополнительный фотон в сигнал со временем задержки, меньшим, чем временное окно датчика [5, с. 406, 15, с.114]. Таким образом, субъект А не может обнаружить этот дополнительный фотон, поскольку на него не срабатывает его датчик. После кодировочной операции, выполняемой субъектом А, злоумышленник перехваты-

вает сигнал снова и отделяет дополнительный фотон. Он может получить полную информацию о кодирующей операции субъекта А, выполнив соответствующее измерение. Такой вариант атаки получил название атаки «Троянского коня с задержкой фотона» [15, с.112]. Для противодействия такого рода атаке, а именно атаке с использованием фотонов других длин волн, чем те, которые используют легитимные пользователи, необходимо установить фильтр сигналов с другими длинами волн на входе своего оборудования. На практике легитимные пользователи должны эксплуатировать фильтр длины волны для фильтрации фонового света, особенно когда в качестве квантового канала используется открытая атмосфера (беспроводной оптический канал). Таким образом, для легитимных пользователей нет проблем предотвратить такую атаку. Для атаки «Троянский конь с задержкой фотона» субъект А должен использовать светоделитель 50/50, для деления каждого сигнала на две части и провести измерения состояний в двух измерительных базисах. Если в оригинальном сигнале есть только один фотон, то сработает только один из датчиков, иначе – сработают оба. Таким образом, атаки типа «Троянский конь» могут быть предотвращены техническими средствами. Но тот факт, что этот класс атак существует, показывает, что безопасность квантовых систем не может гарантироваться только принципами квантовой механики, обязательно применение дополнительных специальных технических средств [15, с.113].

К МПИ, которые связаны с несовершенством оборудования, также относятся атаки разделения числа фотонов (photon number splitting attack – PNS attack) и разделения пучка фотонов (photon beam splitting attack – PBS attack).

Атака замены существующего квантового канала лучшим. Совершенствование PNS- и PBS-атак возможно следующим образом: злоумышленник тайно заменяет квантовый канал с потерями между легитимными пользователями идеальным каналом без потерь (или каналом с гораздо меньшими потерями). В таком случае злоумышленник сможет блокировать определенную часть однофотонных импульсов, выдавая потери за естественные – то есть субъект Б получит примерно такое же количество пустых импульсов, как и до замены канала. Нетрудно заметить, что для начального канала с большими потерями злоумышленник будет иметь возможность получить почти весь ключ и остаться незамеченным. Кроме того, если уровень потерь в первоначальном канале очень значительный, то злоумышленник при замене его на значительно лучший сможет сохранить не только ожидаемую субъектом Б долю пустых импульсов, но и всю статистику числа фотонов в импульсе. Отметим также, что атаку замены существующего квантового канала лучшим, очень трудно осуществить на практике. В любом случае легитимные пользователи для защиты от такого типа атаки должны использовать квантовый канал ограниченной длины так, чтобы коэффициент передачи оставался достаточно высоким [15, с.113].

Методы перехвата информации с использованием утечки информации по побочным каналам. В [33, с.5] также рассмотрена атака, при которой злоумышленник *измеряет пространственные, спектральные или временные характери-*

стики импульсов, передаваемых беспроводным оптическим каналом. Проанализированные в этой работе эксперименты с протоколом BB84 показывают, что наибольшее количество информации о передаваемых битах ключа, $6{,}6\times10^{-3}$ бит/импульс, злоумышленник может получить при измерении спектральных характеристик. Но эта величина достаточно мала и из этого следует, что атаку нельзя считать мощной. Другая атака, связанная с временной несбалансированностью детектора (timing channel attack), в отличие от предыдущих методов, позволяет злоумышленнику получить значительную часть секретного ключа. Технические методы защиты от этой атаки также предложены в [34, с.38].

В целом, в настоящее время теоретические аспекты безопасности квантовой криптографии являются очень активной областью исследований, но их значительно меньше посвящено тщательному изучению практических квантовых систем. Однако в последнее время наблюдается растущий интерес к анализу МПИ с использованием побочных каналов, что является результатом физической реализации методов и систем квантовой криптографии.

В результате проведенных исследований были выявлены возможности реализации угроз, а также уязвимости в системах КК, которые сведены в таблицу 2.1.

Таблица 2.1 - Модель угроз в системах КК

Название	Возможность реализации	Уязвимость детерминистических протоколов	Нарушение характеристик безопасности		
			К	Ц	Д
Coherent	-	+	+	-	-
Non-Coherent	+	+	+	+	-
MithM	+/-	+	-	+	-
DoS	+	+	-	-	+
Trojan Horse	+/-	+	+	-	-
PNS	+	-	+	-	-
PBS	+	-	+	-	-
Channel Change	+/-	+	+	-	-
Timing Channel	+	+	+	-	-

По результатам исследований определено, что детерминистические протоколы уязвимы к ряду специфических атак, из которых наиболее опасной и распространенной является некогерентная атака (Non-Coherent Attack) – строка выделена серым цветом в таблице 2.1. Эта атака направлена на нарушение 2/3 характеристик информационной безопасности согласно модели, Триада КЦД (CIA Triad), а именно нарушению конфиденциальности, и целостности передаваемых данных. Кроме этого, некогерентная атака, в отличие от семейства когерентных атак, например, может быть реализована на существующем оборудовании в со-

ответствии с текущим состоянием развития ИКТ. Исходя из этого, далее в диссертационной работе будет рассматриваться стойкость детерминистических протоколов именно в контексте защищенности от некогерентной атаки.

2.3 Абстрактная модель нарушителя в системах квантовой криптографии

Основной и первоочередной задачей злоумышленника является *несанкционированный доступ* (НСД) к ресурсам ИКС (в данном случае ИКС на основе КТ) с разной целью. Исключением является случай, когда злоумышленник нечаянно реализует НСД – в таком случае он является *случайным нарушителем*, но не злоумышленником. Особую опасность могут нести нарушители, которые находятся под влиянием криминальных группировок, бизнес-структур, политических организаций, спецслужб и т.п. Допустимым характером действий таких нарушителей может быть стремление получения определенных данных для их дальнейшего использования, модификации или уничтожения с целью достижения определенных условий для себя или структур, под влиянием которых они находятся. Стоит также отметить, что нарушитель может быть, как внутренним (из числа сотрудников, например), так и внешним (находится за пределами контролируемой зоны ИКС или проникший в нее несанкционированным путем) [35].

Квалификация нарушителя – совокупность определенных знаний и умений нарушителя, которые он использует для реализации НСД к ресурсам ИКС. Можно отметить несколько типов квалификации нарушителей, которые позволят успешно реализовать угрозы в частности квантовым системам: а) владеет информацией о функциональных особенностях квантовой системы вообще, умеет пользоваться штатными средствами соответственной ИКС; б) нарушитель имеет высокий уровень знаний и опыт работы в техническом обслуживании аналогичных ИКС или квантовых систем; в) обладает высоким уровнем знаний в области вычислительной техники (криптографии, теории алгоритмов, параллельных вычислений и др.) и программирования на языках разработки программного обеспечения для квантовых систем или их аналогов; г) владеет знаниями квантовой физики, квантовой оптики и т.д., а также навыками работы с оборудованием, которое используется в таких системах; д) нарушитель имеет доступ к глобальным вычислительным сетям, суперкомпьютеру или квантовому компьютеру, с помощью чего может реализовать, например, силовую атаку.

Возможности нарушителя относительно влияния на квантовые системы можно представить в виде следующей иерархической классификации [35, с.20]:

1) имеет возможность запуска определенного ограниченного набора программного обеспечения, которое реализует определенные функции по обработке классической или квантовой информации;

2) может создавать собственное программное обеспечение и модифицировать существующее, что позволит создать новые функции обработки классической и квантовой информации для последующего получения части требуемой информации;

3) имеет возможность управлять функционированием квантовой системы, т.е. непосредственно влиять на программное обеспечение, состав и конфигурацию технического обеспечения ИКС;

4) имеет весь объем возможностей легитимных пользователей – может разрабатывать и внедрять в эксплуатацию технические средства ИКС, а также интегрировать собственные технические средства с целью последующего получения полезной ему информации.

Подчеркнем, что теоретический анализ стойкости квантовых протоколов, как правило, производится исходя из того, что нарушитель имеет технические возможности, ограниченные только законами квантовой механики, а не текущим уровнем развития технологий.

Цели нарушителя в квантовых системах – это создание новых и усовершенствование существующих методов крипто анализа (классических и квантовых). Основой целенаправленной реализации нарушителем НСД к ресурсам ИКС чаще всего являются корыстные мотивы, хотя иногда бывает желание самовыражения или нанесение морального ущерба легитимным пользователям. Нарушитель может использовать совокупность релевантных знаний, умений и навыков, например: а) знание математического аппарата позволит ему создать новые методы криптоанализа в соответствии с текущем уровнем защиты; б) знание языков программирования позволит нарушителю реализовать созданные методы криптоанализа, а также модифицировать существующее программное обеспечение легитимных пользователей; в) знание квантовой физики даст возможность подобрать соответствующие МПИ (см. рисунок 2.2) и получить полезную информацию; г) знание методов социального инжиниринга может позволить нарушителю без основательных знаний математики, физики и программирования легко обойти системы ЗИ как классические, так и квантовые [35, с.21].

По *характеру действий* нарушителей можно классифицировать следующим образом: 1) случайный нарушитель, который ошибочно, нечаянно и бессознательно нарушил политику безопасности ИКС; 2) терпеливый нарушитель, который нарушил политику безопасности определенного сегмента или всей ИКС сознательно, намеренно, но без решительных действий, маскируясь, подбирая атрибуты доступа легитимных пользователей с целью преодоления средств управления доступом и т.д.; 3) решительный злоумышленник, цель которого нарушить одну из характеристик информационных ресурсов ИКС. Он стремится преодолеть все существующие средства ограничения доступа и получить возможность непосредственного доступа к ресурсам ИКС с целью вмешательства в работу системы, модификации или уничтожения информации (классической или квантовой), получения необходимых данных и т.д.; 4) удаленный нарушитель, анализирует технические каналы утечки информации, удаленно влияет с помощью специальных средств на локальные и распределенные ИКС, включая квантовый и классический каналы (см. рисунок 2.3).

Рисунок 2.3 – Схема реализации МПИ в системах КРК [35, с.21]

Для более подробного построения модели нарушителя, исходя из конкретной ИКС (в т.ч. зависимо от особенностей квантовой системы – протоколов, длины квантового канала, технических характеристик оборудования, а также наличия дополнительных технических средств ЗИ), рекомендуется также классифицировать нарушителей по следующим признакам: по подготовке к преодолению системы физической защиты ИКС; по характеру поведения; по уровню информированности об объекте атаки; по используемым методам и средствам; по месту реализации атаки и др.

Предложенные в работе модели угроз и нарушителя в системах КРК позволяют четко определить направления дальнейших исследований по разработке методов усиления секретности и усовершенствованию квантовых систем ЗИ. Кроме этого, они позволяют сформировать концептуальные аспекты модели предупреждения атак и формализовать возможности превентивных систем (в процессе их разработки или усовершенствования). Разработанная модель нарушителя в квантовых системах позволяет определить совокупность мероприятий различного характера, которые необходимо дополнительно внедрять для обеспечения надежной защиты при использовании специфических квантовых систем [35, с.20].

2.4 Особенности реализации некогерентной атаки в системах квантовой криптографии на базе детерминистических протоколов

Проанализируем некогерентную атаку пассивного перехвата на детерминистический протокол с использованием вспомогательных квантовых систем [5, с.,16, 36-39]. Согласно работе [38, с.5] субъект *Е* не имеет информации о кутрите, заранее подготовленным субъектом Б и хранимый в его квантовой памяти в течение одного цикла протокола, поэтому перехваченный переданный кутрит по пути следования от субъекта *А* к субъекту *Б,* даже после измерения его состояния, не даст ему никакую информацию. Состояние «передаваемого» кутрита

полностью смешанное – его редуцированная матрица плотности имеет следующий вид:

$$\rho_{red} = \frac{1}{3}\left(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|\right). \qquad (2.2)$$

Субъект Е может воспользоваться вспомогательными квантовыми системами (пробами) в случае с кутритами, также, как и для протокола с парами перепутанных кубитов. Пробы перемешиваются в соответствии с алгоритмом с передаваемым кутритом на пути его следования от субъекта *Б* к субъекту *А* (см. рисунок 2.4). Затем субъект *Е* выполняет измерения над составной квантовой системой «передаваемый кутрит – проба» на пути от субъекта *А* к субъекту *Б*.

Согласно теореме расширения Стайнспринга [17, с. 2, 38, с.7], операция субъекта *Е* на линии субъект *Б* $\rightarrow$ субъект *А* (см. рисунок 2.3) может быть реализована унитарным оператором в гильбертовом пространстве проб H_E, размерность которого удовлетворяет условию $dimH_E \leq (dimH_B)^2$, где H_B – размерность гильбертова пространства передаваемого субъектом *Б* кутрита $(dimH_B=3)$.

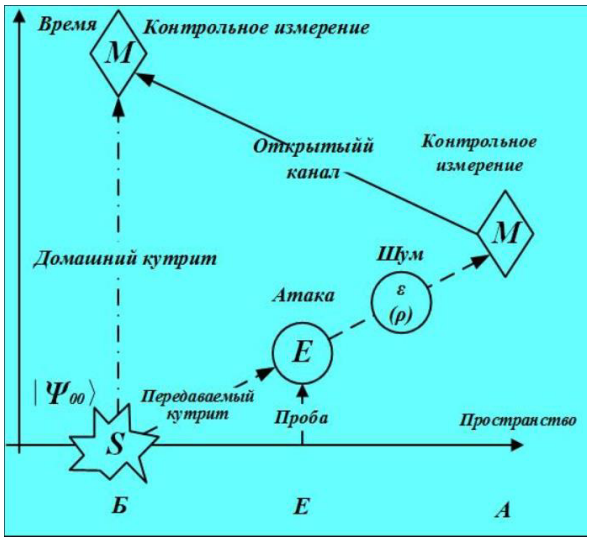


Рисунок 2.4 – Схема некогерентной атаки пассивного перехвата на детерминистический протокол с парами перепутанных кутритов

Таким образом, субъект *Е* может, в частности, использовать для атаки пробы, состоящие из одного $(dimH_E=3)$ или двух $(dimH_E=9)$ кутритов. Некогерентная атака с использованием двух кутритных проб *является более общей и соответственно более сильной*, потому проанализируем эту атаку.

Состояние передаваемого кутрита полностью смешанное и аналогично кубитовому протоколу можно считать, что субъект *Б* посылает кутрит в одном из состояний, $|0\rangle$, $|1\rangle$ или $|2\rangle$ (добавляется третье состояние) с вероятностью $1/3$ -

состояния составной системы «передаваемый кутрит – проба субъекта *E*» после атаки могут быть записаны так:

$$\begin{aligned} \left|\psi^{(0)}\right\rangle &= \hat{E}\left|0,\varphi\right\rangle = \alpha_0|0,\varphi_{00}\rangle + \beta_0|1,\varphi_{01}\rangle + \gamma_0|2,\varphi_{02}\rangle; \\ \left|\psi^{(1)}\right\rangle &= \hat{E}\left|1,\varphi\right\rangle = \alpha_1|0,\varphi_{10}\rangle + \beta_1|1,\varphi_{11}\rangle + \gamma_1|2,\varphi_{12}\rangle; \\ \left|\psi^{(2)}\right\rangle &= \hat{E}\left|2,\varphi\right\rangle = \alpha_2|0,\varphi_{20}\rangle + \beta_2|1,\varphi_{21}\rangle + \gamma_2|2,\varphi_{22}\rangle\ , \end{aligned} \qquad 2.3)$$

где $\{|\varphi_{ij}\rangle\}, i,j = 0 \ldots 2$ – множество состояний пробы субъекта *E*.

Атакующая операция представлена в виде матрицы:

$$\hat{E} = \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \\ \gamma_0 & \gamma_1 & \gamma_2 \end{bmatrix}. \qquad (2.4)$$

Между параметрами проб субъекта *E* в соответствии с условиями унитарности операции $\hat{E}$ следуют соотношения :

$$\alpha_i^*\alpha_j + \beta_i^*\beta_j + \gamma_i^*\gamma_j = \delta_{ij}, \qquad (2.5)$$

где δ_{ij} – символ Кронекера, *i, j* = 0…2.

Из-за полностью смешанного состояния передаваемого кутрита должны быть выполнены соотношения:

$$|\alpha_0|^2 = |\beta_1|^2 = |\gamma_2|^2; \qquad |\alpha_1|^2 = |\beta_2|^2 = |\gamma_0|^2; \qquad |\alpha_2|^2 = |\beta_0|^2 = |\gamma_1|^2. \qquad (2.6)$$

Когда субъект *Б* «посылает $|0\rangle$» состояние системы «передаваемый кутрит – проба субъект *E*» после атаки $\hat{E}$ становиться $\left|\psi^{(0)}\right\rangle$ (2.3). После выполнения субъектом *A* кодирующих операций U_{00}, U_{10}, U_{20}, U_{01}, … (таблица 2.2) с частотами p_{00}, p_{10}, p_{20}, p_{01}, … соответственно, оператор плотности системы «передаваемый кутрит – проба субъекта *E*» будет таким:

$$\rho^{(0)} = \sum_{i,j=0}^{2} p_{ij}\left|\psi_{ij}^{(0)}\right\rangle\left\langle\psi_{ij}^{(0)}\right|, \qquad (2.7)$$

где $$\left|\psi_{00}^{(0)}\right\rangle = U_{00}\left|\psi^{(0)}\right\rangle = \alpha_0|0\rangle|\varphi_{00}\rangle + \beta_0|1\rangle|\varphi_{01}\rangle + \gamma_0|2\rangle|\varphi_{02}\rangle,$$

$$\left|\psi_{10}^{(0)}\right\rangle = U_{10}\left|\psi^{(0)}\right\rangle = \alpha_0|0\rangle|\varphi_{00}\rangle + \beta_0 e^{2\pi i/3}|1\rangle|\varphi_{01}\rangle + \gamma_0 e^{4\pi i/3}|2\rangle|\varphi_{02}\rangle,$$

$$\left|\Psi_{20}^{(0)}\right\rangle = U_{20}|\psi^{(0)}\rangle = a_0|0\rangle|\varphi_{00} + \beta_0 e^{4\pi i/3}\left|1\right\rangle|\varphi_{01}\rangle + \gamma_0 e^{2\pi i/3}\left|2\right\rangle|\varphi_{02}\rangle$$

$$\left|\psi_{01}^{(0)}\right\rangle = U_{20}\left|\psi^{(0)}\right\rangle = \alpha_0|1\rangle|\varphi_{00}\rangle + \beta_0|2\rangle|\varphi_{01}\rangle + \gamma_0|0\rangle|\varphi_{02}\rangle,$$

$$\left|\psi_{11}^{(0)}\right\rangle = U_{11}\left|\psi^{(0)}\right\rangle = \alpha_0|1\rangle|\varphi_{00}\rangle + \beta_0 e^{2\pi i/3}|2\rangle|\varphi_{01}\rangle + \gamma_0 e^{4\pi i/3}|0\rangle|\varphi_{02}\rangle,$$

$$\left|\psi_{21}^{(0)}\right\rangle = U_{21}\left|\psi^{(0)}\right\rangle = \alpha_0|1\rangle|\varphi_{00}\rangle + \beta_0 e^{4\pi i/3}|2\rangle|\varphi_{01}\rangle + \gamma_0 e^{2\pi i/3}|0\rangle|\varphi_{02}\rangle,$$

$$\left|\psi_{02}^{(0)}\right\rangle = U_{02}\left|\psi^{(0)}\right\rangle = \alpha_0|2\rangle|\varphi_{00}\rangle + \beta_0|0\rangle|\varphi_{01}\rangle + \gamma_0|1\rangle|\varphi_{02}\rangle,$$

$$\left|\psi_{12}^{(0)}\right\rangle = U_{12}\left|\psi^{(0)}\right\rangle = \alpha_0|2\rangle|\varphi_{00}\rangle + \beta_0 e^{2\pi i/3}|0\rangle|\varphi_{01}\rangle + \gamma_0 e^{4\pi i/3}|1\rangle|\varphi_{02}\rangle,$$

$$\left|\psi_{22}^{(0)}\right\rangle = U_{12}\left|\psi^{(0)}\right\rangle = \alpha_0|2\rangle|\varphi_{00}\rangle + \beta_0 e^{4\pi i/3}|0\rangle|\varphi_{01}\rangle + \gamma_0 e^{2\pi i/3}|1\rangle|\varphi_{02}\rangle. \qquad (2.8)$$

Максимальная классическая информация I_0, доступная субъекту E после измерения над составной системой «передаваемый кутрит – проба», определяется энтропией Холево [10, с.75, 17, с.3]:

$$I_0 = S\left(\rho^{(0)}\right) - \sum_{i,j=0}^{2} p_{ij} S\left(\rho_{ij}^{(0)}\right) = S\left(\rho^{(0)}\right), \qquad (2.9)$$

где $\rho_{ij}^{(0)} = \left|\psi_{ij}^{(0)}\right\rangle\left\langle\psi_{ij}^{(0)}\right|$; S – энтропия фон Неймана и все $S\left(\rho_{ij}^{(0)}\right)$ равны нулю, т.к. состояния (2.8) при выполнении условий (2.5) – чистые. Таким образом,

$$I_0 = S\left(\rho^{(0)}\right) \equiv -Tr\left\{\rho^{(0)}\log_3\rho^{(0)}\right\} = -\sum_i \lambda_i \log_3 \lambda_i \quad \text{(трит)}, \qquad (2.10)$$

где λ_i – собственные значения оператора плотности $\rho^{(0)}$ (2.7).

Величина I_0 показывает, сколько информации может получить субъект E после финального измерения над составной системой. Для нахождения собственных значений λ_i оператора плотности $\rho^{(0)}$ (2.7), этот оператор был записан в матричном виде в следующем ортогональном базисе (2.11). С помощью системы Wolfram Mathematica 7 [36, с.6] были определены уравнения девятой степени для собственных значений матрицы плотности и возможное разложение на произведение трех кубических уравнений вида (2.12):

$$\left\{|0,\varphi_{00}\rangle, |1,\varphi_{00}\rangle, |2,\varphi_{00}\rangle, |0,\varphi_{01}\rangle, |1,\varphi_{01}\rangle, |2,\varphi_{01}\rangle, |0,\varphi_{02}\rangle, |1,\varphi_{02}\rangle, |2,\varphi_{02}\rangle\right\}. \qquad (2.11)$$

$$\lambda^3 - (p_{00} + p_{10} + p_{20})\lambda^2 + 3\left(|\alpha_0|^2|\beta_0|^2 + |\alpha_0|^2|\gamma_0|^2 + |\beta_0|^2|\gamma_0|^2\right)\times$$

$$\times(p_{00}p_{10}+p_{00}p_{20}+p_{10}p_{20})\lambda-27|\alpha_0|^2|\beta_0|^2|\gamma_0|^2p_{00}p_{10}p_{20}=0;$$

$$\lambda^3-(p_{01}+p_{11}+p_{21})\lambda^2+3\left(|\alpha_0|^2|\beta_0|^2+|\alpha_0|^2|\gamma_0|^2+|\beta_0|^2|\gamma_0|^2\right)\times$$

$$\times(p_{01}p_{11}+p_{01}p_{21}+p_{11}p_{21})\lambda-27|\alpha_0|^2|\beta_0|^2|\gamma_0|^2p_{01}p_{11}p_{21}=0;$$

$$\lambda^3-(p_{02}+p_{12}+p_{22})\lambda^2+3\left(|\alpha_0|^2|\beta_0|^2+|\alpha_0|^2|\gamma_0|^2+|\beta_0|^2|\gamma_0|^2\right)\times$$

$$\times(p_{02}p_{12}+p_{02}p_{22}+p_{12}p_{22})\lambda-27|\alpha_0|^2|\beta_0|^2|\gamma_0|^2p_{02}p_{12}p_{22}=0. \qquad (2.12)$$

Аналогично рассматриваются другие случаи в (2.3), т.е. когда субъект *Б* вместо $|0\rangle$ «посылает» $|1\rangle$ или $|2\rangle$. В этих случаях собственные значения матриц плотности $\rho^{(1)}$ и $\rho^{(2)}$, с учетом соотношений (2.6), определяются теми же уравнениями. Поскольку при симметричной атаке $|\alpha_0|^2|\beta_0|^2=|\alpha_0|^2|\gamma_0|^2=(1-d_z)d_z/2$, $|\beta_0|^2|\gamma_0|^2=\frac{d_z^2}{4}$ и $|\alpha_0|^2|\beta_0|^2|\gamma_0|^2=(1-d_z)\frac{d_z^2}{4}$, то уравнения (2.12) принимают вид:

$$\lambda^3-(p_{00}+p_{10}+p_{20})\lambda^2+3\left(d_z-\frac{3}{4}d_z^2\right)(p_{00}p_{10}+p_{00}p_{20}+p_{10}p_{20})\lambda-$$

$$-\frac{27}{4}\left(d_z^2-d_z^3\right)p_{00}p_{10}p_{20}=0; \qquad (2.13)$$

$$\lambda^3-(p_{01}+p_{11}+p_{21})\lambda^2+3\left(d_z-\frac{3}{4}d_z^2\right)(p_{01}p_{11}+p_{01}p_{21}+p_{11}p_{21})\lambda-$$

$$-\frac{27}{4}\left(d_z^2-d_z^3\right)p_{01}p_{11}p_{21}=0; \qquad (2.14)$$

$$\lambda^3-(p_{02}+p_{12}+p_{22})\lambda^2+3\left(d_z-\frac{3}{4}d_z^2\right)(p_{02}p_{12}+p_{02}p_{22}+p_{12}p_{22})\lambda-$$

$$-\frac{27}{4}\left(d_z^2-d_z^3\right)p_{02}p_{12}p_{22}=0. \qquad (2.15)$$

На рисунке 2.5 приведены зависимости I_0 от d_z при симметричной атаке субъекта *Е* и различных значениях частот p_{00}, …, p_{22} кодирующих операций субъекта *А* (таблицы 2.2 - 2.3). Для получения этих зависимостей уравнения (2.13) – (2.15) решались численно при определенных значениях p_{00}, …, p_{22} и полученные девять значений $\lambda_1,\ldots,\lambda_9$ подставлялись в (2.10). Как видно из рисунка 2.5, для большинства наборов частот p_{00}, …, p_{22} количество информации субъекта *Е* монотонно возрастает с ростом вероятности обнаружения атаки d_z и достигает максимума при $d_z=2/3$. Это значение d_z можно считать максимальным, поскольку при $d_z>2/3$ количество информации субъекта *Е* начинает убывать (на

графиках не показано). Соответственно, субъект *E* не будет выбирать параметры своих проб, от которых зависит d_z, так, чтобы d_z превышало $2/3$ – для субъекта *E* не имеет смысла увеличивать вероятность обнаружения атаки при уменьшении доступной ему информации. Также из рисунка 2.5 видно, что максимальное количество информации I_0 субъекта *E*, который соответствует $d_z = 2/3$, равно энтропии источника при любых значениях частот p_{00}, …, p_{22}. Это означает, что при $d_z = 2/3$ и только при таком значении d_z субъект *E* получит полную информацию (при симметричной атаке). Также факт равенства I_0 и *H* при $d_z = 2/3$ свидетельствует о правильной асимптотики формул (2.15).

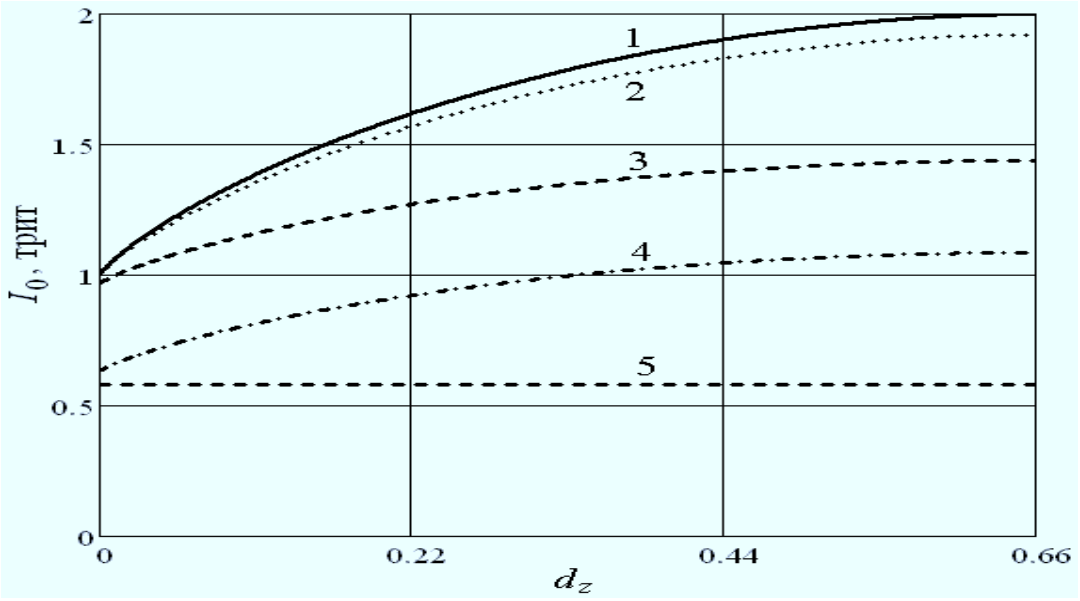


Рисунок 2.5 – Зависимость количества информации I_0 субъекта *E* от вероятности d_z обнаружения атаки при симметричной атаке [36, с.8]

Таблица 2.2 – Частоты p_{00}, …, p_{22} тритовых биграмм

№ кривой на рис. 2.5	p_{00}	p_{10}	p_{20}	p_{01}	p_{11}	p_{21}	p_{02}	p_{12}	p_{22}
1	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9
2	1/6	1/9	1/18	1/6	1/18	1/9	1/18	1/9	1/6
3	2/9	0	2/9	0	2/9	0	2/9	0	1/9
4	0.4	0.1	0	0	0.4	0.1	0	0	0
5	2/3	0	0	0	1/3	0	0	0	0

Отметим также, что полученная зависимость количества информации субъекта *E* от вероятности обнаружения атаки при контроле подслушивания в одном базисе для протокола с парами перепутанных кутритов (см. рисунок 2.5) анало-

гична соответствующей зависимости для протокола с парами перепутанных кубитов, за исключением того, что максимальная вероятность обнаружения атаки при однократном контроле в протоколе с кутритами равна $2/3$, а в протоколе с кубитами – равна $1/2$.

Таблица 2.3 – Энтропия источника $H = -\sum_{i,j=0}^{2} p_{ij} \log_3 p_{ij}$ (трит/биграмма)

№ кривой на рис. 2.5	H
1	2.000
2	1.921
3	1.439
4	1.086
5	0.579

Таким образом, использование кутритов вместо кубитов в детерминистическом протоколе позволяет не только увеличить информационную емкость протокола, но и увеличить вероятность обнаружения атаки пассивного перехвата при контроле подслушивания [40].

Из рисунка 2.5 видно также, что при $d_z = 0$ количество информации субъекта E не равно нулю, однако оно ниже своего максимального значения при $d_z = 2/3$. Таким образом, для детерминистического протокола с перепутанными парами кутритов существует «невидимый» режим подслушивания, при котором субъект E получает часть информации, но его операции не могут быть обнаружены легитимными пользователями, при использовании в режиме контроля подслушивания только одного измерительного базиса. Отметим, что аналогичная ситуация имеет место и для детерминистического протокола с парами перепутанных кубитов. Как показывают расчеты проф. Василиу Е.В. в работе [38, с.6], условие унитарности атакующей операции субъекта E приводит к важной зависимости между d_z и d_x, а именно: *вне зависимости от значения одной из этих величин другая всегда равна своему максимальному значению*. Таким образом, при использовании двух измерительных базисов в режиме контроля подслушивания «невидимого» режима подслушивания уже не существует и детерминистический протокол с парами перепутанных кутритов имеет асимптотическую стойкость к атаке пассивного перехвата, аналогично протоколу с парами перепутанных кубитов.

Таким образом, во втором разделе диссертации разработаны модель угроз и модель нарушителя в квантово-криптографических системах, которые учитывают специфику и уязвимости систем КК, а также возможности нарушителей в соответствии с текущим и перспективным уровнем вычислительных технологий. Данные модели позволяют определить и выбрать наиболее защищенные методы распределения криптографических ключей. В частности, модель угроз позволяет сформировать концептуальные аспекты предупреждения атак и формализовать возможности превентивных систем в процессе их разработки или усовершенствования. Абстрактная модель нарушителя в системах КК позволяет определить

совокупность мероприятий различного характера, необходимые для дополнительного внедрения в специфические квантовые системы для обеспечения надежной защиты.

Кроме этого, на основе существующих исследований, рассмотрена детально некогерентная атака на детерминистический протокол с кутритами в силу уязвимости и асимптотической стойкости этой категории протоколов, с целью учета этих особенностей для построения эффективных моделей и методов распределения ключей в последующих разделах диссертации.

3 МОДЕЛИ БЕЗОПАСНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА БАЗЕ ДЕТЕРМИНИСТИЧЕСКОГО ПРОТОКОЛА КВАНТОВОЙ КРИПТОГРАФИИ

Квантовая криптография, основанная на теории квантовой механики, позволяет развивать новые методы обеспечения устойчивости и безопасности передачи информации, решать проблемы классической криптографии, связанной с распределением ключей [28, с.3, 39, 41]. Кроме того, позволяет обеспечить устойчивость к различного рода квантовым алгоритмам поиска ключей [6, с.155]. Применение квантовых детерминистических протоколов позволяет решать проблемы обеспечения секретности передачи сообщений без применения шифрования. Данная секретность гарантируется законами квантовой физики [6, с.75, 10, с.75]. С помощью квантовых состояний групп квантовых систем (двух- или многоуровневых, часто применяются фотоны) кодируется исходный текст секретного сообщения, далее он передается квантовым каналом связи. Законы квантовой физики также гарантируют обнаружение подслушивания в канале. Поэтому во время сеанса связи легитимные пользователи (А и Б) могут сразу обнаружить нарушителя (Е) и прервать сеанс связи. Для практической реализации детерминистического протокола [17, с.4] достаточно небольшого объема квантовой памяти, и реализация на основе существующего технического оборудования. Данный вариант протокола использует два состояния Белла перепутанной пары кубитов, что позволяет передавать за один цикл протокола один бит классической информации [5, с.13]. Если же использовать все четыре состояния пары кубитов Белла, т. е. квантовое сверхплотное кодирование, тогда возможно увеличение количества битов за цикл в два раза, то есть уже будет два бита [6, с.109]. Для наращивания информационной емкости вместо перепутанных пар кубитов можно использовать уже их тройки, четверки т.д. В частности, работа [40, с.118] исследует протокол с перепутанными состояниями Гринбергера – Хорна - Цайлингера (ГХЦ) троек и четверок кубитов. Эти состояния обеспечивают информационную емкость равную n битов на цикл, то есть количество кубитов в используемых состояниях ГХЦ.

Также для наращивания информационной емкости протокола можно использовать перепутанные состояния многоуровневых квантовых систем. Например, в [33-34, с.23] исследован протокол с использованием состояний Белла пары трехуровневых систем (кутритов) и квантового сверхплотного кодирования для кутритов. Его информационная емкость составляет бит на цикл, а не два бита на цикл как для протокола Белла с состояниями кубитов. В [42-48] рассматриваются различные виды атак, проанализирована общая некогерентная атака для различных вариантов протокола, в том числе для протокола с парами кутритов. При атаке нарушитель Е может снять некоторое количество информации, прежде чем эта атака будет обнаружена [47]. В работе [48, с. 257] исследован метод обратного хеширования сообщения, основанный на умножении на случайные обратные матрицы. Итоговое перемноженное сообщение передается по квантовому

каналу, в это же время легитимные пользователи имеют возможность проанализировать уровень ошибок, применив режим контроля подслушивания протокола. Так, например, в случае если не превышается допустимый уровень, то по классическому (не квантовому) каналу передают сами матрицы, вторая сторона в итоге может получить исходный текст, путем умножения полученного сообщения на соответствующие обратные матрицы. Рассматриваемая модель протокола позволяет сравнивать уровни ошибок с определенным средним уровнем шума, излучаемого квантовым каналом и по результату сравнения, сделать заключение о наличии, либо об отсутствии факта прослушивания.

Исследования [7, с. 39, 48, с. 258] подтверждают высказывания о том, что уровни ошибок, вызываемых действиями нарушителя и природных шумов в канале, имеют не простой характер. В связи с этим возникает проблема с синхронизацией регистрации изменений в состояниях передаваемых фотонов, возникающих от совместного влияния естественного шума в канале и действий нарушителя. Дальнейшие исследования позволят создать модель, имитирующую работу протокола в режиме контроля подслушивания и получить ряд практических рекомендаций по применению квантового протокола в канале с шумом.

3.1 Детерминистический протокол квантовой криптографии с использованием пар кутритов

Согласно [47] существует девять полностью перепутанных ортонормированных состояний пары кутритов $|\Psi_{00}\rangle \ldots |\Psi_{22}\rangle$ (таблица 3.1), которые образуют базис в гильбертовом пространстве двух кутритов и являются обобщением состояний Белла на кутриты [47, с. 24]. Эти состояния превращаются друг в друга под действием локального унитарного оператора на любой один из кутритов пары. Предположим, что начальным состоянием, которое готовит принимающая сторона – субъект *Б*, является $|\Psi_{00}\rangle$. Тогда необходимо построить набор унитарных операций над одним из двух кутритов в состоянии $|\Psi_{00}\rangle$, преобразующих это состояние в состояния $|\Psi_{00}\rangle \ldots |\Psi_{22}\rangle$ соответственно (над вторым кутритом при этом не нужно проводить никаких операций, т.е. можно сказать, что на него действует тождественный оператор). Также в таблице 3.1 приведены строки из двух тритов, которые будут соответствовать каждому из состояний $|\Psi_{00}\rangle \ldots |\Psi_{22}\rangle$. О таком соответствии (методе квантового кодирования классической информации) субъекты *А* и *Б* должны договориться до начала протокола.

Приведем теперь пошаговое описание детерминистического протокола с использованием пар полностью перепутанных кутритов [36, с.5, 48-54].

Отправитель сообщения (субъект *А)* заранее разбивает свою строку кутритов на пары кутритов. Если сообщение изначально является битовой строкой, то его необходимо преобразовать в строку кутритов.

Шаг 1. Субъект *Б* готовит пару кутритов в состоянии $|\Psi_{00}\rangle$, используя, например, экспериментальный метод, предложенный в [55-57]. В этом случае

кутрит является одиночным фотоном, три ортогональных состояния которого являются состояниями с различным орбитальным угловым моментом, а пара таких кутритов-фотонов перепутывается по их орбитальным угловым моментам.

Таблица 3.1 – Квантовое кодирование классической информации для детерминистического протокола с перепутанными парами кутритов [49, с.25]

Состояние $\left\|\Psi_{ij}\right\rangle$	Оператор U_{ij} для преобразования $\left\|\Psi_{00}\right\rangle$ в $\left\|\Psi_{ij}\right\rangle$, действующий на второй кутрит	Пара тритов
$\left\|\Psi_{00}\right\rangle = \left(\left\|00\right\rangle + \left\|11\right\rangle + \left\|22\right\rangle\right)/\sqrt{3}$	$U_{00} = \left\|0\right\rangle\left\langle 0\right\| + \left\|1\right\rangle\left\langle 1\right\| + \left\|2\right\rangle\left\langle 2\right\|$	00
$\left\|\Psi_{10}\right\rangle = \left(\left\|00\right\rangle + e^{2\pi i/3}\left\|11\right\rangle + e^{4\pi i/3}\left\|22\right\rangle\right)/\sqrt{3}$	$U_{10} = \left\|0\right\rangle\left\langle 0\right\| + e^{2\pi i/3}\left\|1\right\rangle\left\langle 1\right\| + e^{4\pi i/3}\left\|2\right\rangle\left\langle 2\right.$	10
$\left\|\Psi_{20}\right\rangle = \left(\left\|00\right\rangle + e^{4\pi i/3}\left\|11\right\rangle + e^{2\pi i/3}\left\|22\right\rangle\right)/\sqrt{3}$	$U_{20} = \left\|0\right\rangle\left\langle 0\right\| + e^{4\pi i/3}\left\|1\right\rangle\left\langle 1\right\| + e^{2\pi i/3}\left\|2\right\rangle\left\langle 2\right\|$	20
$\left\|\Psi_{01}\right\rangle = \left(\left\|01\right\rangle + \left\|12\right\rangle + \left\|20\right\rangle\right)/\sqrt{3}$	$U_{01} = \left\|1\right\rangle\left\langle 0\right\| + \left\|2\right\rangle\left\langle 1\right\| + \left\|0\right\rangle\left\langle 2\right\|$	01
$\left\|\Psi_{11}\right\rangle = \left(\left\|01\right\rangle + e^{2\pi i/3}\left\|12\right\rangle + e^{4\pi i/3}\left\|20\right\rangle\right)/\sqrt{3}$	$U_{11} = \left\|1\right\rangle\left\langle 0\right\| + e^{2\pi i/3}\left\|2\right\rangle\left\langle 1\right\| + e^{4\pi i/3}\left\|0\right\rangle\left\langle 2\right\|$	11
$\left\|\Psi_{21}\right\rangle = \left(\left\|01\right\rangle + e^{4\pi i/3}\left\|12\right\rangle + e^{2\pi i/3}\left\|20\right\rangle\right)/\sqrt{3}$	$U_{21} = \left\|1\right\rangle\left\langle 0\right\| + e^{4\pi i/3}\left\|2\right\rangle\left\langle 1\right\| + e^{2\pi i/3}\left\|0\right\rangle\left\langle 2\right\|$	21
$\left\|\Psi_{02}\right\rangle = \left(\left\|02\right\rangle + \left\|10\right\rangle + \left\|21\right\rangle\right)/\sqrt{3}$	$U_{02} = \left\|2\right\rangle\left\langle 0\right\| + \left\|0\right\rangle\left\langle 1\right\| + \left\|1\right\rangle\left\langle 2\right\|$	02
$\left\|\Psi_{12}\right\rangle = \left(\left\|02\right\rangle + e^{2\pi i/3}\left\|10\right\rangle + e^{4\pi i/3}\left\|21\right\rangle\right)/\sqrt{3}$	$U_{12} = \left\|2\right\rangle\left\langle 0\right\| + e^{2\pi i/3}\left\|0\right\rangle\left\langle 1\right\| + e^{4\pi i/3}\left\|1\right\rangle\left\langle 2\right\|$	12
$\left\|\Psi_{22}\right\rangle = \left(\left\|02\right\rangle + e^{4\pi i/3}\left\|10\right\rangle + e^{2\pi i/3}\left\|21\right\rangle\right)/\sqrt{3}$	$U_{22} = \left\|2\right\rangle\left\langle 0\right\| + e^{4\pi i/3}\left\|0\right\rangle\left\langle 1\right\| + e^{2\pi i/3}\left\|1\right\rangle\left\langle 2\right\|$	22

Шаг 2. Субъект *Б* оставляет у себя первый кутрит («домашний») и посылает субъекту *А* второй («передаваемый») по квантовому каналу связи, например, оптоволоконной линии (см. рисунок 3.1).

Шаг 3. Субъект *А* получает «передаваемый» кутрит от субъекта *Б*. С вероятностью *q* он переходит в режим контроля подслушивания и выполняется шаг 4, иначе субъект *А* переходит в режим передачи сообщения и тогда выполняются шаги с 5-го по 7-ой.

Шаг 4. Контроль подслушивания выполняется квантовыми измерениями состояний кутритов. При этом состояние каждого из кутритов измеряется отдельно – одного субъектом *А*, другого субъектом *Б*, а измерения, как и для детерминистического протокола с кубитами, необходимо выполнять в двух различных базисах, переключаясь между ними случайным образом. В случае применения только одного измерительного базиса для контроля подслушивания субъект *Е* имеет возможность так подобрать параметры своих вспомогательных квантовых систем, используемых для атаки, что легитимные пользователи не обнаружат его операций.

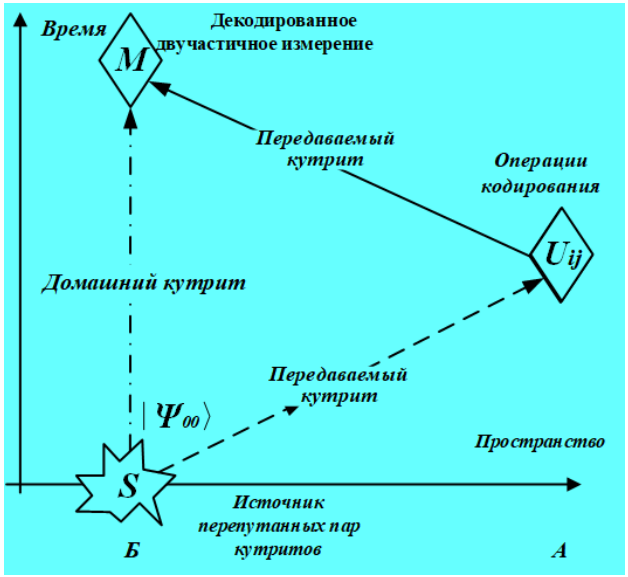


Рисунок 3.1 – Режим передачи сообщения детерминированным протоколом [55, с.153]

Лучше всего для контроля подслушивания использовать взаимно несмещенные (дополнительные) базисы, для которых любые два базисных вектора, относящиеся к разным базисам, удовлетворяют соотношению $\langle e_i | e_j \rangle = 1/\sqrt{d}$, где d – размерность гильбертова пространства квантовой системы ($d = 3$ для кутритов).

Для кутритов существуют четыре взаимно несмещенных базиса, из которых два называются z-базисом и x-базисом [6, с. 53, 58], а другие два v-базисом и t-базисом, что описано (2.16) – (2.19).

Субъект A может выбрать для контроля подслушивания любые два из этих четырех базисов. Использование трех или всех четырех базисов не увеличит вероятность обнаружения подслушивания.

Для режима контроля подслушивания была вычислена таблица результатов измерений субъектов A и $Б$ во всех четырех базисах. Результат удобнее представить не в виде таблицы, а записав исходное состояние $|\Psi_{00}\rangle$ в базисах (2.16) – (2.19):

$$|\Psi_{00}\rangle = \big(|00\rangle + |11\rangle + |22\rangle\big)/\sqrt{3} = \big(|x_0x_0\rangle + |x_1x_2\rangle + |x_2x_1\rangle\big)/\sqrt{3} = \\ = \big(|t_0v_0\rangle + |t_1v_1\rangle + |t_2v_2\rangle\big)/\sqrt{3} = \big(|v_0t_0\rangle + |v_1t_1\rangle + |v_2t_2\rangle\big)/\sqrt{3}. \qquad (3.1)$$

После выбора двух базисов для контроля подслушивания субъектом A, субъект $Б$ также должен выбрать два базиса, но его выбор обусловлен выбором субъекта A, как видно из (3.1). Так, если субъект A выбрал z-базис или x-базис, то субъект $Б$ должен также выбрать z-базис или x-базис. А если субъект A выбрал, например, x-базис и v-базис, то субъект $Б$ должен выбрать x-базис и t-базис. Субъекты A и $Б$ могут договориться о том, какие базисы они будут использовать,

до начала протокола, чтобы заранее наладить свою аппаратуру, хотя такая предварительная договоренность, в принципе, не является обязательной.

Таким образом, в режиме контроля подслушивания субъект *А* выбирает случайно один из двух взаимно несмещенных базисов и измеряет в этом базисе состояние полученного от субъекта *Б* кутрита. Затем он сообщает субъекту *Б* по классическому открытому каналу результат измерения и использованный базис (см. рисунок 3.2). В любом из базисов субъект *А* получит один из трех возможных результатов измерения с одинаковой вероятностью. Затем субъект *Б*, выбрав соответствующий базис и выполнив измерения состояния своего «домашнего» кутрита, должен получить определенный результат (с вероятностью 1), согласно (3.1). Так, например, если субъект *А* выбрал *x*-базис и получил результат «1», то субъект *Б* должен тоже выбрать *x*-базис и его результат должен быть «2». Или, например, если субъект *А* выбрал *v*-базис и получил результат «0», то, согласно (3.1), субъект *Б* должен выбрать *t*-базис и получить результат «0». Аналогично из (3.1) можно получить все другие возможные варианты измерений.

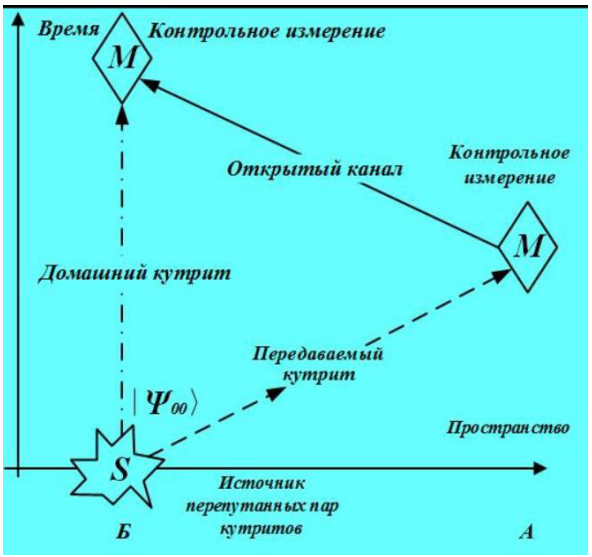


Рисунок 3.2 – Детерминистический квантовый протокол в режиме контроля подслушивания [55, с.153]

Если результат измерения субъекта *Б* правильный, то подслушивания нет. Субъект *Б* сообщает об этом субъекту *А* по классическому каналу, и они переходят к шагу 1 протокола. Если результат измерения субъекта *Б* неверный, то принимается решение о наличии подслушивания и протокол прерывается.

Отметим, что если результат измерения субъекта *Б* неверный, то это может свидетельствовать о вмешательстве субъекта *Е*, или об ошибках, возникающих при передаче кутритов по квантовому каналу связи. Поскольку не существует способа различить ошибки, возникающие по этим двум причинам [6, с.17], то в квантовом канале с шумом протокол необходимо усовершенствовать. В этом подразделе рассмотрен детерминистический протокол с кутритами только для

идеального квантового канала, обобщение этого протокола, как и других вариантов детерминистического протокола, для квантового канала с помехами изложено в пп. 3.2-3.4 диссертации.

Отметим также, что классический канал, по которому субъекты *А* и *Б* обмениваются сообщениями в режиме контроля подслушивания, может быть открытым для пассивного прослушивания и нет необходимости шифровать сообщения, передаваемые этим каналом. Однако субъект *Е* не должен иметь возможности изменять сообщения, передаваемые в классическом канале, иначе, контролируя также и квантовый канал, он может провести атаку типа «человек посередине». Таким образом, легитимные пользователи должны обеспечивать кодом аутентичности все сообщения, передаваемые в классическом канале.

Шаг 5. В соответствии со своей текущей двухтритовой строкой, субъект *А* выбирает одну из девяти кодирующих операций (таблица 3.1) и выполняет эту операцию над кутритом, полученным им от субъекта *Б*. При этом исходное состояние пары кутритов $|\Psi_{00}\rangle$ изменится в соответствии с операцией, выполненной субъектом *А*. Затем субъект *А* отправляет кутрит назад субъекту *Б* по квантовому каналу (см. рисунок 3.2).

Шаг 6. Получив «передаваемый» кутрит от субъекта *А*, субъект *Б* выполняет декодирующие измерения над парой кутритов в базисе Белла для кутритов, что позволяет ему достоверно определить состояние, созданное кодирующей операцией субъекта *А*, и тем самым определить двухтритовую строку, которую послал субъект *А*. Набор проекционных операторов для измерений в базисе Белла для кутритов содержит девять операторов: $\left\{|\Psi_{ij}\rangle\langle\Psi_{ij}|\right\}$, где $i, j = 0\ldots2$, а все девять $|\Psi_{ij}\rangle$ заданы в таблице 3.1.

Шаг 7. Если сообщение передано полностью, то протокол успешно завершен, в противном случае переходим к *шагу* 1.

3.2 Модель квантового детерминистического протокола в режиме контроля подслушивания

Взяв за основу исследования, проводимые в [17, с.7, 36, с.6], а именно поведение детерминистического протокола в канале с шумом, можно сделать вывод, что в режиме контроля подслушивания протокола (рисунок 3.2) оба пользователя осуществляют проверку на неизменность первоначальных перепутанных состояний заготовленных вторым пользователем $|\Psi_{00}\rangle = \left(|00\rangle + |11\rangle + |22\rangle\right)/\sqrt{3}$, так как атака нарушителя на канал внесет изменения в эти состояния.

Оба пользователя замеряют состояние каждого кутрита отдельно друг от друга, причем это измерение проводится в двух различных базисах, переключаемых случайным образом. Примером, может служить два взаимно несмещенных базиса *z* и *x*:

$$|z_0\rangle = |0\rangle,\ |z_1\rangle = |1\rangle,\ |z_2\rangle = |2\rangle;$$

$$|x_0\rangle = \left(|0\rangle + |1\rangle + |2\rangle\right)/\sqrt{3},\ |x_1\rangle = \left(|0\rangle + e^{2\pi i/3}|1\rangle + e^{-2\pi i/3}|2\rangle\right)/\sqrt{3},$$

$$|x_2\rangle = \left(|0\rangle + e^{-2\pi i/3}|1\rangle + e^{+2\pi i/3}|2\rangle\right)/\sqrt{3} \qquad (3.1)$$

С вероятностью равной $^{1/3}$ пользователь А в каждом из базисов получит один из трех возможных результатов – «0», «1» или «2». В свою очередь пользователь Б после получения результатов замера с выбранным базисом также замеряет состояния своего заготовленного, «домашнего» кутрита (рисунок 3.1).

Так в работе [36, с.3] доказано что, пользователь Б с вероятностью равной 1 может получить результат, это следует из записи состояния $|\Psi_{00}\rangle$ в z - и x- базисах:

$$|\Psi_{00}\rangle = \left(|00\rangle + |11\rangle + |22\rangle\right)/\sqrt{3} = \left(|x_0x_0\rangle + |x_1x_2\rangle + |x_2x_1\rangle\right)/\sqrt{3}. \qquad (3.2)$$

Однако точные результаты замеров пользователь Б может получить только в случае, когда в квантовом канале отсутствуют как естественная помеха или шум, так и атака нарушителя. Способа распознавания таких ошибок, когда в канале присутствуют и естественные помехи, и помехи, возникающие от действий нарушителя Е, пока нет. В связи с этим проблема построения модели, позволяющей исследовать совместную атаку нарушителя и природного квантового шума в канале, является актуальной.

Природа квантового канала может иметь множество ошибок, связанных с изменением фазы или вращением в гильбертовом пространстве квантового состояния кубита. Основным и важным свойством квантового кода, исправляющего некоторое дискретное множество ошибок является способность автоматически исправлять непрерывное множество ошибок. Данное свойство объясняется измерением синдрома ошибки или проектированием состояния с малой ошибкой на состояние без ошибки, либо проектированием ложного состояния на какое-либо состояние большей части ошибок дискретного множества. Иначе говоря, имеет место дискретизация квантовых ошибок, позволяющая формировать квантовые коды для исправления некоторого дискретного множества ошибок, причем исправлять любую ошибку автоматически в состоянии квантовых систем [6, с.19].

Работа канала заключается в следующем: с вероятностью p состояние кубита становится полностью смешанным, т.е. деполяризуется, а с вероятностью $(1-p)$ оно остается неизменным. Из работы [11, с. 529] следует: оператор деполяризованного канала для кубитов описывается уравнением:

$$\varepsilon(\rho) = (1-p)\rho + p/3 \cdot \left(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z\right). \qquad (3.3)$$

Оператор σ_x - описывает «классическую» ошибку переворота кубита, оператор σ_z - описывает ошибки переворота фазы, а оператором σ_y - описываются ком-

бинации этих двух ошибок, фазовые ошибки. Деполяризованный канал воздействует на кубит как суперпозиция этих трех крупных дискретных квантовых ошибок.

Хотя деполяризованный канал не может передать все потенциально возможные виды квантовых ошибок, но может учесть существенные из большинства дискретных квантовых ошибок [11, с.534]. Итак, данный канал широко используется в квантовой теории информации как модель квантового шума.

В соответствии с [57, с. 48, 58, с. 8,] действие деполяризованного канала отдельного кутрита описывается оператором:

$$\varepsilon_{qutrit}(\rho) = (1-p)\rho + p/8 \cdot \left(Y\rho Y^{\dagger} + Z\rho Z^{\dagger} + Y^2\rho\left(Y^2\right)^{\dagger} + YZ\rho(YZ)^{\dagger} + Y^2Z\rho\left(Y^2Z\right)^{\dagger} + \right.$$
$$\left. + YZ^2\rho\left(YZ^2\right)^{\dagger} + Y^2Z^2\rho\left(Y^2Z^2\right)^{\dagger} + Z^2\rho\left(Z^2\right)^{\dagger}\right), \qquad (3.4)$$

где $Y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{2\pi i/3} & 0 \\ 1 & 0 & e^{4\pi i/3} \end{pmatrix}$.

На рисунке 3.2 представлен режим контроля подслушивания детерминистического протокола с парами перепутанных кутритов для случая, когда на передаваемый кутрит действует оператор шума (3.4). На передаваемый кутрит первоначально воздействует атака нарушителя, затем воздействует оператор шума. В соответствии с проведенным анализом по схеме работы [6, с.23] и обобщением ее на протокол с парами кутритов, приведенном в работе [11, с.471], состояние квантовой системы «передаваемый кутрит - проба нарушителя» после совершенной атаки нарушителя можно представить в виде:

$$\left|\psi^{(0)}\right\rangle = E\left|0,\varphi\right\rangle = \alpha_0\left|0,\varphi_{00}\right\rangle + \beta_0\left|1,\varphi_{01}\right\rangle + \gamma_0\left|2,\varphi_{02}\right\rangle,$$
$$\left|\psi^{(1)}\right\rangle = E\left|1,\varphi\right\rangle = \alpha_1\left|0,\varphi_{10}\right\rangle + \beta_1\left|1,\varphi_{11}\right\rangle + \gamma_1\left|2,\varphi_{12}\right\rangle, \qquad (3.5)$$
$$\left|\psi^{(2)}\right\rangle = E\left|2,\varphi\right\rangle = \alpha_2\left|0,\varphi_{20}\right\rangle + \beta_2\left|1,\varphi_{21}\right\rangle + \gamma_2\left|2,\varphi_{22}\right\rangle.$$

В итоге комбинированного состояния передаваемого кутрита можно условно принять, что пользователь Б отправляет кутрит в виде либо состояния $|0\rangle$, либо $|1\rangle$, либо $|2\rangle$ с вероятностью равной $1/3$. В формулах (3.5) *(i,j=0)*$\{\left|\varphi_{ij}\right\rangle\}$ *(i,j=0…2)* представлено множество состояний кутритов – пробы нарушителя Е.

Атакующее действие нарушителя Е может быть представлено в виде матрицы:

$$E = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \\ \gamma_0 & \gamma_1 & \gamma_2 \end{pmatrix}. \qquad (3.6)$$

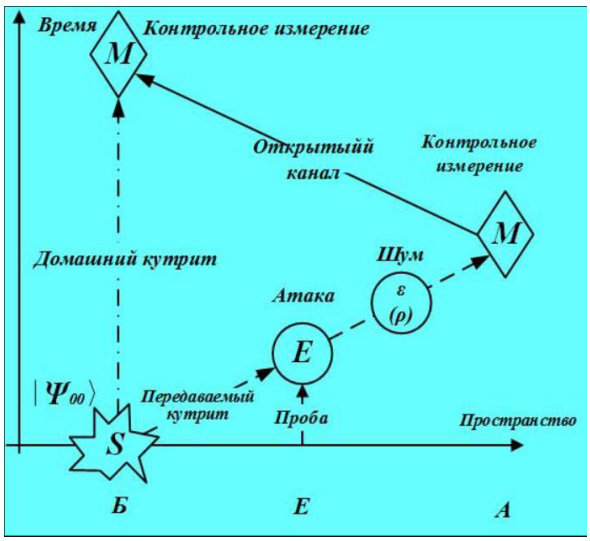


Рисунок 3.3 – Режим контроля подслушивания в деполяризованном канале при некогерентной атаке [48, с.10]

В случае, когда пользователь Б отправляет $|0\rangle$, то состояние передаваемого кутрита после комбинированной операции нарушителя Е представится в виде:

$$|\psi\rangle = \alpha_0|0\rangle + \beta_0|1\rangle + \gamma_0|2\rangle, \tag{3.7}$$

а его матрица плотности в базисе состояний $|0\rangle, |1\rangle, |2\rangle$:

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha_0|^2 & \alpha_0\beta_0^* & \alpha_0\gamma_0^* \\ \beta_0\alpha_0^* & |\beta_0|^2 & \beta_0\gamma_0^* \\ \gamma_0\alpha_0^* & \gamma_0\beta_0^* & |\gamma_0|^2 \end{pmatrix}. \tag{3.8}$$

После преобразования (3.4) с подстановкой (3.8) получим:

$$\rho_{out} = \frac{1}{8}\begin{pmatrix} \left(3p\left(|\beta|^2 + |\gamma|^2\right) + (8-6p)|\alpha|^2\right) & (8-9p)\alpha\beta^* & (8-9p)\alpha\gamma^* \\ (8-9p)\beta\alpha^* & \left(3p\left(|\alpha|^2 + |\gamma|^2\right) + (8-6p)|\beta|^2\right) & (8-9p)\beta\gamma^* \\ (8-9p)\gamma\alpha^* & (8-9p)\gamma\beta^* & \left(3p\left(|\alpha|^2 + |\beta|^2\right) + (8-6p)|\gamma|^2\right) \end{pmatrix} \tag{3.9}$$

Индексы «0» α, β и γ для сокращения записи далее не рассматриваются. R_z вероятность ошибочного результата равна сумме двух других диагональных элементов (либо разности между единицей и левым верхним элементом матрицы ρ_{out}) то есть:

$$R_z = 1 - 1/8 \cdot \left(3p\left(|\beta|^2 + |\gamma|^2\right) + (8-6p)|\alpha|^2\right). \tag{3.10}$$

R_z свидетельствует об изменении состояния передаваемого кутрита, при измерении в z - базисе пользователем Б.

Вероятность обнаружения атаки нарушителя Е во время реализации протокола в идеальном квантовом канале согласно работе [36, с.9] равна:

$$d_z = |\beta|^2 + |\gamma|^2 = 1 - |\alpha|^2 . \qquad (3.11)$$

Преобразуя выражение (3.10) с помощью (3.11), получим:

$$R_z = d_z + \frac{3}{4} p\left(1 - \frac{3}{2} d_z\right) . \qquad (3.12)$$

Результат (3.12) не изменится даже в том случае, когда на передаваемый кутрит будет воздействовать шум, и следом атака нарушителя Е. Расчеты свидетельствуют, что диагональные элементы матрицы плотности (3.9) не зависят от того, кто внес помехи в первую очередь, либо атака операций нарушителя Е, либо помехи самого деполяризованного канала.

В случаях, когда пользователь Б отправляет $|1\rangle$ или $|2\rangle$, это соответствует волновым функциям $|\psi^{(1)}\rangle$ и $|\psi^{(2)}\rangle$ в (3.5), тогда с из-за соотношения между параметрами согласно работе [36, с.7]:

$$|\alpha_0|^2 = |\beta_1|^2 = |\gamma_2|^2; |\alpha_1|^2 = |\beta_2|^2 = |\gamma_0|^2; |\alpha_2|^2 = |\beta_0|^2 = |\gamma_1|^2 . \qquad (3.13)$$

Эти случаи будут также иметь результат выражения (3.12). Таким образом, полная вероятность ошибки при измерении пользователя Б в базисе z будет:

$$R_{полна-z} = \frac{1}{3} \cdot 3R_z = R_z = d_z + \frac{3}{4} \cdot p\left(1 - \frac{3}{2} d_z\right). \qquad (3.14)$$

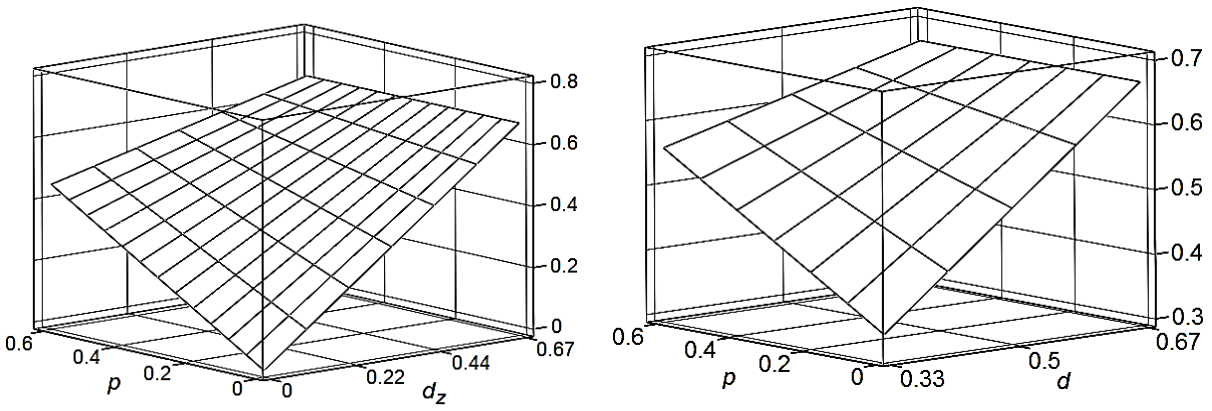
Аналогично можно выполнить такие же расчеты для контрольного измерения пользователя Б в базисе x, получим идентичную структуру выражения для вероятности ошибки $R_{полна-x}$:

$$R_{полна} = d_x + \frac{3}{4} p\left(1 - \frac{3}{2} d_x\right) , \qquad (3.15)$$

где d_x - вероятность ошибки при измерении пользователем Б в базисе x при реализации детерминистического протокола в идеальном квантовом канале.

Согласно работе [36, с.9] максимальное значение, соответствующее полной информации нарушителя Е равно 2/3. На рисунке 3.4 а приведена зависимость $R_{полна-z}$ от d_z и p. Из рисунка 3.4 а следует, что суперпозиция операции нарушителя

Е и шума в деполяризованном канале приводит к тому, что при $d_z=2/3$ $R_{полна\text{-}z}$ не зависит от p и так же равна 2/3.



а) б)

Рисунок 3.4 – Зависимости полной вероятности ошибки при измерении пользователя Б в одном из базисов (а) и средней вероятности ошибки в двух базисах (б) для ДПК [48, с.10]

Из полученных результатов следует, что при некогерентной атаке максимальное значение вероятности ошибки при выполнении протокола в режиме контроля подслушивания в деполяризованном канале будет одинаковой как с шумом, так и без него.

В базисе x атака нарушителя создает максимальный уровень $d_x=2/3$, независимо от уровня ошибок d_z, создаваемого им в базисе z, и так же наоборот [36, с.10]. На рисунке 3.4 б показана зависимость:

$$R_{полна} = 1/2 \cdot \left(2/3 + R_{полна-z}\right), \tag{3.16}$$

от p и среднего уровня ошибок, создаваемых атакой, по обоим базисам: $d = 1/2 \cdot \left(2/3 + d_z\right)$, при условии, что легитимные пользователи переключаются между базисами z- и x- с равной вероятностью 1/2, что является для них наиболее разумной стратегией контроля подслушивания [36, с.11, 48, с.10].

3.3 Формализация системы помехоустойчивого кодирования над полем Галуа GF (3^2) для кутритов

Так как в реальных квантовых каналах имеются помехи, то для практической реализации КПБС нужны коды, позволяющие их исправлять. В настоящее время разработаны семейства квантовых помехоустойчивых кодов, исправляющих непосредственно искажённые в канале квантовые состояния [11, с.527]. Однако, практическое применение таких кодов требует использования квантовых логических гейтов [6, с.29, 11, с.41], с технологической точки зрения это пока

достаточно сложно и нерационально. Поскольку КПБС предназначен для безопасной передачи классической информации по квантовым каналам связи, то для кодирования классической информации можно использовать классические помехоустойчивые коды непосредственно до ее передачи посредством квантовых частиц. В протоколах с группами *n* перепутанных кубитов информация передается пакетами по *n* бит, поэтому будут возникать и пачки ошибок соответствующей длины. В теории двоичных кодов, исправляющих пачки ошибок, в настоящее время разработано достаточно большое количество двоичных помехоустойчивых кодов [59-62], отличающихся избыточностью и корректирующей способностью. Одними из таких кодов являются коды Рида-Соломона (РС-коды), применяемые для передачи в классических каналах с высокой интенсивностью помех. Использование протоколов с парами перепутанных кутритов позволяет увеличить информационную емкость, и как следствие, скорость передачи информации. Поэтому обеспечение ее безошибочной передачи такими протоколами является актуальной задачей, которую можно решить с помощью троичных РС-кодов. В [63] подробно описаны троичные РС-коды и установлена корректирующая способность при передаче информации с использованием в квантовом канале с шумом перепутанных пар кутритов.

Для моделирования работы системы КПБС необходимо формализовать математический аппарат кодов в соответствии с [59, с. 240, 60, с. 111, 63, с.45]. Пусть *a* - элемент поля $GF(q^m)$ порядка *n,* где *q, m* - целые числа, причем $q>1$, $m>0$ и $q^m \neq 2$. Если *a* - примитивный элемент, то его порядок равен (q^m-1), то есть $a^{q^m-1}=1$ и $a^i \neq 1$, где $0<i<(q^m-1)$. Тогда нормированный полином *g(x)* минимальной степени над полем $GF(q^m)$, решениями которого является $(d-1)$ степеней a^{i_0}, a^{i_0+1}, …, a^{i_0+d-2}элемента *a*, является порождающим полиномом РС-кодов над полем $GF(q^m)$: $g(x) = (x-a^{i_0})(x-a^{i_0+1})\ldots(x-a^{i_0+d-2})$, где i_0 – некоторое целое число, с помощью которого иногда удается упростить процедуру кодирования (часто $i_0=1$). Длина полученного кода $n=q^m-1$ символов и содержит $r=d-1=deg(g(x))$ проверочных символов, где *deg()* означает степень полинома, а *d* – минимальное кодовое расстояние (минимальное из всех расстояний Хемминга всех пар кодовых символов). Число информационных символов $k = n - r = n - d+1$. Таким образом, $d = n - k+1$. РС-коды исправляют $t = r/2$ ошибок, но требуют $r=2t$ проверочных символов. С их помощью исправляются произвольные пачки ошибок длиной не более *t*.

Процедура кодирования. Для получения закодированного полинома *C(x)* необходимо к информационному полиному *S(x)* добавить $2t=r$ проверочных символов так, чтобы *C(x)* делился на *g(x)* без остатка. Кодирование может быть реализовано двумя способами: систематическим и несистематическим. При несистематической кодировке выполняется перемножение *S(x)* с *g(x)*: $C(x) = S(x)\,g(x)$, полученный закодированный полином полностью отличается от первоначального и для извлечения из него *S(x)* нужно сначала выполнить операцию декодирования (несмотря на отсутствие ошибок). Такой способ кодирования требует больших затрат ресурсов только на изъятие информационного полинома *S(x)*,

при этом он может быть без ошибок. При систематическом кодировании при отсутствии ошибок в $C(x)$ для получения информационного полинома $S(x)$ нужно лишь отбросить $2t=r$ последних символа [55, с.151].

Систематическое кодирование происходит следующим образом [55, с.152]:

1) К $S(x)$ приписывается $2t=r$ нулей, получается полином: $T(x) = S(x)\, x^{2t}$.

2) Полином $T(x)$делится на порождающий полином $g(x)$, находится остаток $R(x)$: $T(x) = S(x)\, x^{2t} = Q(x)g(x)+R(x)$, где $Q(x)$- частное.

3) На основе остатка определяется корректирующий РС-код, для этого из полинома $T(x)$ нужно вычесть $R(x)$. И так, кодовое сообщение примет вид: $C(x)= Q(x)g(x)= T(x)- R(x)= S(x)\, x^{2t}- R(x)$.

Процедура декодирования. Пусть во время передачи на закодированный полином $C(x)$ подействовал шум $e(x)$: $Y(x)= C(x) + e(x)$. Для восстановления полинома $C(x)$ и информационного полинома $S(x)$ из полученного $Y(x)$ нужно выполнить операции [55, с.152]:

1) Вычислить синдром ошибки

Для вычисления синдрома ошибки $S(x)$, кодовое слово $Y(x)$ делят на $g(x)$. Если остаток равен нулю, кодовое слово считают не искаженным, то есть $e(x)=0$ и при систематическом кодировании не нужно проводить полную процедуру декодирования, можно просто отбросить проверочные символы и получить информационный полином $S(x)$. Ненулевой остаток свидетельствует о наличии хотя бы одной ошибки. Остаток от деления дает многочлен, не зависящий от $Y(x)$ и который определяется исключительно характером ошибки. Компоненты синдрома ошибки можно вычислить по формуле, $s_i=Y(a^i)$, где $i=1, \ldots, 2t$, причем $s_0=0$. Полученные компоненты объединены в синдром ошибки следующим образом:$s(x)=\overline{s_{2t}s_{2t-1}\ldots s_2 s_1 s_0}$. Если все $s_i=0$ при $i=1, \ldots, 2t$, то $e(x)=0$ и $Y(x)=C(x)$.

2) Вычисление локатора ошибки

Полученный синдром описывает характер ошибки, но не указывает на ее положение. Для этого нужно вычислить локатор ошибки $L(x)$, коэффициенты которого прямо соответствуют коэффициентам искаженных символов. Если количество искаженных символов не превышает t, между $S(t)$ и $L(x)$ существует следующее соответствие, выражаемое формулой $НОД\,(x^{n-1}, C(x)=L(x))$ и вычисление локатора сводится к задаче нахождения наименьшего общего делителя по алгоритму Евклида. На практике обычно применяют более эффективный алгоритм Берлекэмпа-Месси [60, с. 93].

3) Нахождение корней локатора ошибки

Самым простым путем нахождения корней многочлена $L(x)$ является метод проб и ошибок, известный как алгоритм Чиня [60, с.102]. Этот алгоритм состоит в последовательном вычислении $L(a^{-j})$ для каждого $j=1, \ldots, q-1$ и проверки полученных значений на ноль. Если величина $L(a^{-k})$ равна нулю, то a^k является взаимным к корню многочлена локаторов ошибок и k-й элемент кодовой комбинации содержит ошибку.

4) Определение характера ошибки

Используя синдром ошибки и найденные корни локатора ошибок с помощью алгоритма Форни определяется характер ошибки и строится корректирующий полином. Для этого нужно выполнить следующую последовательность операций: а) вычисление многочлена значений ошибок $W(x)$:$W(x)=s(x)L(x) \bmod x^{2t}$; б) нахождение производной многочлена локатора ошибок $L(x)$; в) нахождение корректирующего полинома e': $e' = W(X-1)L'(X_L^{-1})$

5) Исправление ошибки

Корректирующий полином накладывается на кодовое слово и ложные искаженные символы восстанавливаются: $C(x) = Y(x) + e'(x)$. После этого из $C(x)$ отбрасываются проверочные символы и восстанавливается информационный полином $S(x)$.

Так как при передаче информации по квантовому каналу вероятность возникновения ошибок достаточно велика, то были выбраны РС-коды над полем Галуа $GF(3^2)$, у которых $k=r$, что позволяют исправлять $t=n/4$ пар ошибочных тритов. При таких параметрах высокий уровень избыточности, однако исправляется большое количество ошибок. Также было выбрано значение $m=2$, тогда $n=q^m-1=3^2-1=9-1=8$ пар тритов, минимальное кодовое расстояние $d=5$, проверочных символов $r=d-1=5-1=4$ пары тритов, число информационных символов $k= n - r=8 - 4=4$ пары тритов, количество ошибок, которые удастся исправить $t=r/2=2$ пары тритов. Кодирование и декодирование выполнялось над простым полиномом x^2+x+2 в соответствии [55, с.152, 63, с.47], где данные процессы представлены более детально.

3.4 Модель квантового детерминистического протокола в режиме передачи сообщений

Рассмотрим подробно режим передачи сообщения [55, с.153] детерминистическим протоколом с парами полностью перепутанных кутритов (см. рисунок 3.1) [17, с.3, 55, с.153]. Субъект А заранее разбивает свою строку тритов на пары тритов. Если его сообщение изначально является бинарной строкой, то ее необходимо преобразовать в строку тритов.

Далее, согласно [55, с.153], выполняются следующие шаги:

1) Субъект Б готовит пару кутритов в начальном состоянии:

$$|\Psi_{00}\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}.$$

В этом случае кутрит является одиночным фотоном, а пара таких кутритов – фотонов перепутывается по их орбитальному угловому моменту.

2) Субъект Б оставляет у себя первый кутрит («домашний») и отправляет первому пользователю второй («передаваемый») квантовым каналом связи (в качестве которого может использоваться одномодовая оптоволоконная линия или открытое пространство – оптический беспроводной канал).

3) Субъект А получает кутрит переданный субъектом Б. С вероятностью q он переходит в режим контроля подслушивания и выполняется шаг 4, иначе субъект А переходит в режим передачи сообщения и выполняются шаги с 5 по 7.

4) Контроль подслушивания выполняется так называемыми одно частичными квантовыми измерениями состояний кутритов одновременно субъектами А и Б в различных базисах, подробно описано в работе [47, с.7].

5) Субъект А в соответствии со своей текущей двухтритовой строкой, выбирает одну из девяти (с кутритами) кодирующих операций и с помощью квантовых логических гейтов выполняет эту операцию над кутритом, полученным от субъекта Б.

При этом, исходное состояние пары кутритов $|\Psi_{00}\rangle$ изменится в соответствии с выполненной операцией субъекта А [32, с.22]. Затем субъект А квантовым каналом отправляет кутрит назад субъекту Б (см. рисунок 3.4).

6) Субъект Б, получив кутрит переданный субъектом А, выполняет декодирующее двучастичное измерение над парой кутритов в базисе Белла – это позволяет ему достоверно определить состояние, созданное кодирующей операцией субъектом А, и тем самым определить двутритовую строку, им отправленную.

7) Если сообщение передано полностью, то протокол успешно закончен, иначе происходит переход к шагу 1.

Любая система связи подвержена действиям шумов, которые приводят к некорректному приему сигнала. Помехоустойчивое кодирование -высокоэффективное средство решения данной проблемы, основано на введении искусственной избыточности в передаваемые сообщения.

На рисунке 3.5 изображена структурно-логическая модель работы системы КПБС в режиме передачи сообщений по детерминистическому протоколу с применением РС-кодов для кутритов [55, с.152].

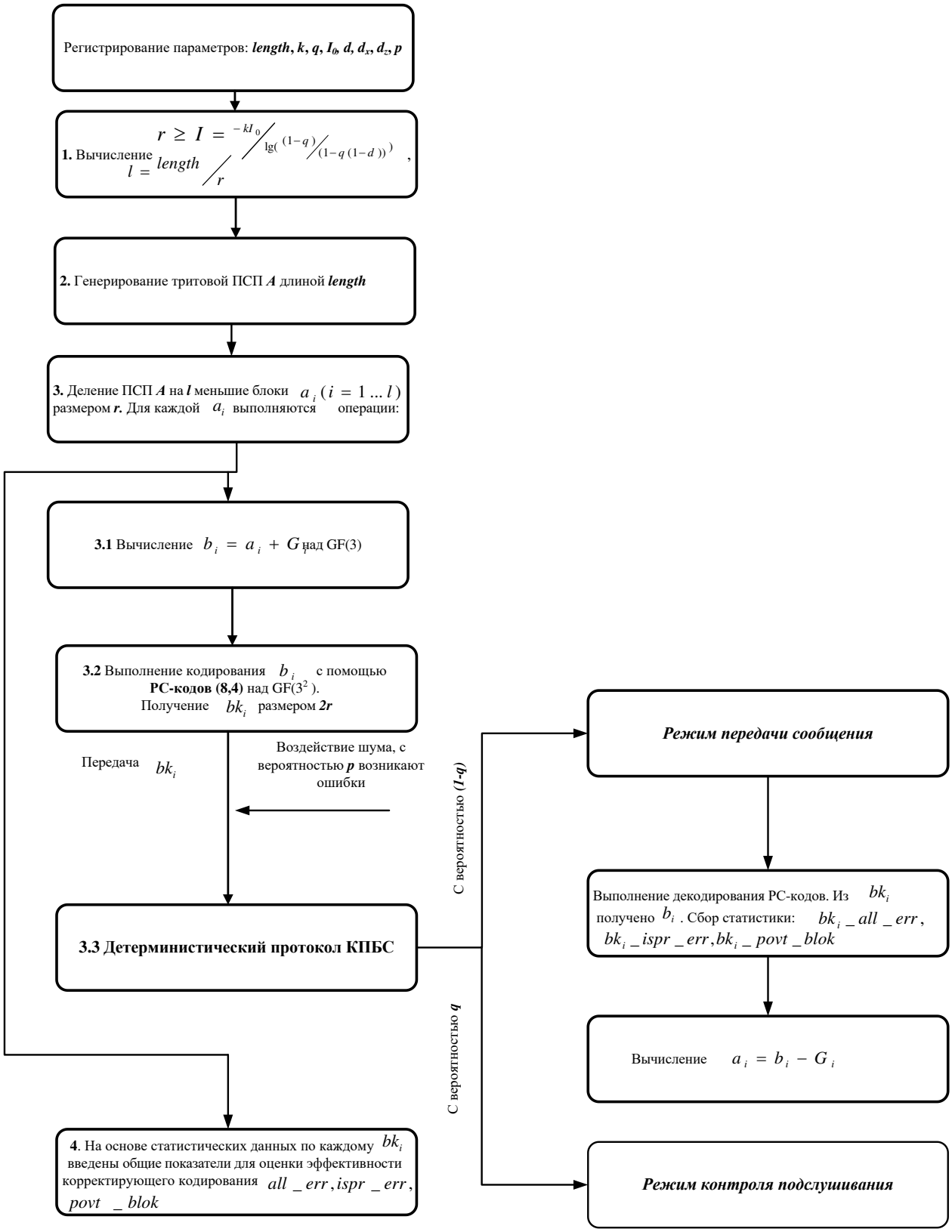


Рисунок 3.5 – Структурно-аналитическая модель работы системы КПБС в режиме передачи сообщений с применением РС-кодов для кутритов [55, с.154]

Оригинальный детерминистический протокол имеет лишь асимптотическую стойкость, поэтому для усиления уровня безопасности системы предлагается применить один из методов усиления [47-52, с.811, 64-69] – умножение на троичную матрицу (подобно шифру Хилла) [70] или на троичную псевдослучайную последовательность [17, с., 71].

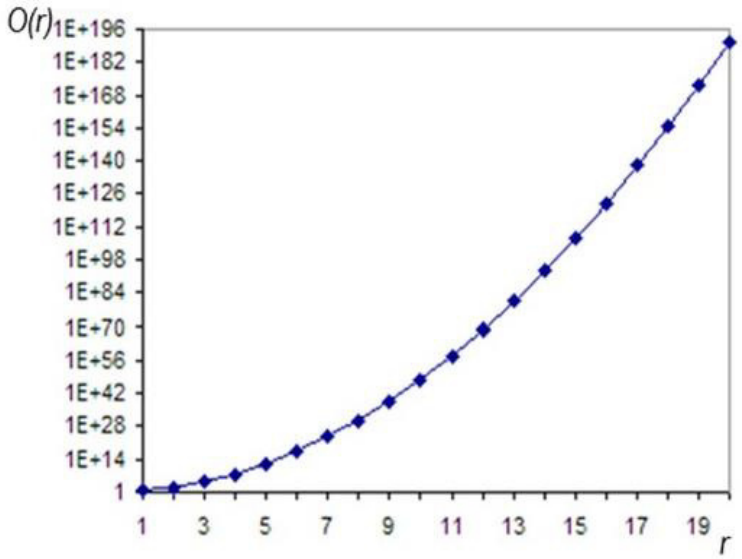


Рисунок 3.6 – Оценка стойкости методов усиления к лобовой атаке

На рисунке 3.6 приведен график, который характеризирует стойкость предложенных методов, то есть зависимость количества необходимых операций для подбора последовательностей (матриц) от непосредственной длины этих последовательностей (размера матриц).

3.5 Подход к усилению секретности детерминистических протоколов квантовой криптографии с использованием пар кутритов

Поскольку один из наиболее эффективных методов усиления секретности [72-73] детерминистических протоколов с парами кутритов заключается в генерировании и дальнейшем использовании (в частности, умножении) обратимых матриц над полем Галуа *GF* (3^2), то актуальной задачей является поиск менее ресурсоемких подходов. Исходя из этого, предлагается использовать троичные ПСЧП [67, с.77, 74].

Описание подхода с учетом последовательности шагов квантового детерминистического протокола [47, с.24, 48, с.8] (пп. 3.1 диссертации):

Перед передачей субъект *A* разбивает свое троичное сообщение на *l* блоков некоторой фиксированной длины *r*, обозначим эти блоки через a_i ($i = 1, \mathrm{K}, l$), затем генерирует для каждого блока отдельно случайную троичную гамму γ_i длиной *r* и складывает полученные гаммы с соответствующими блоками сообщения: $b_i = a_i \oplus \gamma_i$. Полученные в результате блоки b_i передаются по квантовому каналу с использованием детерминистического протокола. Даже если злоумышленнику

удастся перехватить один (или несколько) из этих блоков, оставаясь не обнаруженным, то, не зная использованных гамм γ_i, он не сможет восстановить исходные блоки a_i. Для обеспечения достаточного уровня безопасности длина блока *r* и соответственно размер гамм должны выбираться таким образом, чтобы после передачи одного блока вероятность не обнаружения атаки была пренебрежимо малой величиной. Гаммы γ_i передаются субъекту *Б* по обычному открытому каналу после завершения квантовой передачи, но только в том случае, если легитимные пользователи убедились в отсутствии подслушивания. Затем субъект *Б* складывает их с соответствующими блоками b_i, и восстанавливает исходное сообщение: $a_i = b_i \oplus \gamma_i$.

В соответствии с вышеизложенным методом усиления стойкости детерминистических протоколов для имитационного моделирования протокола с парами перепутанных кутритом разработан алгоритм последовательности действий, который состоит в следующем.

Шаг 1. Сообщение разбивается на *l* блоков a_i заданной длины *r*. Длина блока определяется из условия того, что вероятность не обнаружения атаки после передачи одного блока не превышает заданную величину 10^{-k}:

$$r \geq I = \frac{-kI_0}{\lg((1-q)/(1-q\cdot(1-d)))}, \qquad (3.17)$$

где *I* – количество информации, которое получает злоумышленник при передаче одного блока;

I_0 – количество информации, которое получает злоумышленник за один раунд протокола;

q – вероятность перехода в режим контроля подслушивания;

d – уровень ошибок, вносимый атакой.

Шаг 2. Генерация случайной троичной гаммы γ_i [67, с.77] размером *r* и сложение гаммы с соответствующим блоком $b_i = a_i \oplus \gamma_i$, т.е. выполнение операции *XOR* или *исключающее ИЛИ*.

Шаг 3. Выполнение режима передачи сообщения детерминистического протокола с парами перепутанных кутритов [55, с.155]. Режим контроля подслушивания детерминистического протокола не моделировался.

Шаг 4. В случае, когда легитимные пользователи убедились, что прослушивание отсутствует, происходит передача гамм обычным каналом связи.

Шаг 5. Восстановление исходного блока данных a_i, т.е. сложение полученного блока b_i с соответствующей гаммой γ_i: $a_i = b_i \oplus \gamma_i$. [48, с.10].

3.6 Синтез моделей в единую модель квантового детерминистического протокола с парами перепутанных кутритов

Модели квантового детерминистического протокола с парами перепутанных кутритов [47, с.27] детально описаны в пп. 3.2, 3.4, в частности режимы контроля подслушивания (п. 3.2, изложен с использованием выражений (3.1) – (3.16)) [47-49, с.7, 52, с.813] и передачи сообщений (п. 3.4, шаги 1-7) [48, с. 8, 52, с.812, 55, с.151].

Для эффективного синтеза разработанных моделей, с целью создания комбинированной единой модели детерминистического протокола необходимо более детально рассмотреть такие важные моменты:

1) усиление асимптотической стойкости с учетом вычислительной сложности [50, с.563, 52, с.813, 65-66, с.428, 68-69, с.658];

2) генерирование ПСЧП в поле Галуа *GF* (3^2) [67, с.78, 74, с.207].

Усиление асимптотической стойкости с учетом вычислительной сложности

Процедура усиления стойкости [65-68, с.131] детерминистического квантово-криптографического протокола, которая используется в предложенных моделях, основанная на использовании ПСЧП, требует значительно меньше времени на подготовительную операцию – генерацию ПСЧП в поле *GF* (3^2) заданного размера, чем метод, который использует обратимое хеширование (троичные матрицы) [67, с.79].

Вычисления проводились на двухъядерном процессоре Intel Pentium Dual-Core T3200 со следующими параметрами: тактовая частота (MHz): 2000, частота шины (MHz): 667, кэш 2-го уровня (Kb): 1024, поддерживается набор команд MMX, SSE, SSE2, SSE3, SSSE3, EM64T.

Как видно из рисунка 3.7, генерация одной случайной обратимой матрицы размером 500 ×500 происходит примерно за 6.6 секунд, а для матриц 1000 ×1000 – примерно за минуту (55 секунд). Это время экспоненциально возрастает с увеличением размера матриц. Поэтому, целесообразно использовать предложенный подход усиления стойкости вместо существующего метода, который базируется на матрицах. Таким образом, исходя из рисунка 3.7 использование подхода применения псевдослучайных последовательностей позволит повысить скорость работы комбинированной модели в 22,1 – 36,2 раза для симметричных криптографических систем (при длине ключа 128-256 бит).

Также, отметим, что согласно результатам [73], доля обратимых матриц над полем Галуа *GF*(3^2) составляет 56% (таблица 3.2) от общего количества сгенерированных матриц (при $r \geq 16$).

Атака прямого перебора матриц становится абсолютно невыполнимой (при нынешнем уровне быстродействия вычислительной техники) уже при их размере порядка 16×16, поскольку количество обратимых двоичных матриц такого размера равно $0{,}289 \cdot 2^{256}$, а количество обратимых троичных матриц еще значительно больше: $0{,}56 \cdot 3^{256}$.

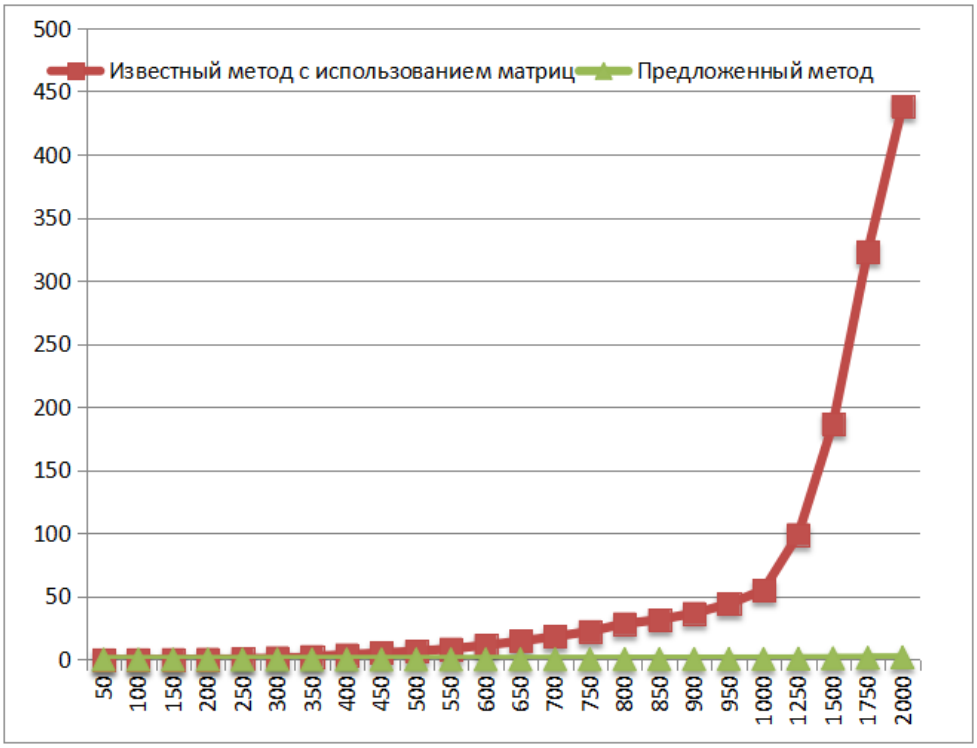


Рисунок 3.7 – Сравнительный анализ вычислительной сложности существующего и предложенных методов усиления стойкости

Таблица 3.2 – Оценки вычислительной стойкости генерации случайных обратимых матриц размера $r \times r$ над полем GF(3^2)

r	Среднее количество обратимых матриц из 1000 сгенерированных	Среднее время генерирования случайных обратимых матриц, с	Среднее время обратного хеширования методом Гаусса, с
50	563	0,3	0,026
100	563	1,4	0,080
150	557	2,9	0,138
200	557	6,1	0,240

Также для генерации случайного ключа субъект *A* может использовать квантовые генераторы случайных чисел, например, квантовый генератор QUANTIS компании IdQuantique [23], приведенный на рисунке 1.5 в первом разделе диссертации, который генерирует истинно случайные числа.

Таким образом, в п. 3.6 диссертационной работы в результате синтеза реализована комбинированная модель на основе разработанных модели режима контроля подслушивания и модели режима передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов с применением предложенного метода усиления секретности. Синтез позволил усовершенствовать метод безопасного распределения ключей, повысить скорость и обеспечить помехоустойчивость деполяризационного квантового канала.

В третьем разделе диссертационной работы были получены следующие важные научные и практические результаты:

1. Разработана модель квантового детерминистического протокола в режиме контроля подслушивания, которая учитывает особенности квантового канала и вероятности возникновения в нем ошибки в x- и z- базисах измерения, энтропию фон Неймана, а также использует новую процедуру усиления секретности, позволяющую обеспечить безопасное и быстрое распределение ключей (в контексте реализации некогерентной атаки), а также сформулировать практические рекомендации по разработке квантово-криптографических систем в условиях использования деполяризационного квантового канала и присутствия нарушителя.

2. Разработана модель квантового детерминистического протокола в режиме передачи сообщений, которая за счет формализации системы помехоустойчивого кодирования над полем Галуа $GF(3^2)$ для кутритов, повышения асимптотической стойкости оригинального детерминистического протокола, а также использования алгоритма генерирования троичных псевдослучайных последовательностей, позволяющего повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом и небольшом уровне природных шумов.

3. Предложен метод усиления секретности с использованием квантовых перепутанных состояний и сгенерированных троичных псевдослучайных последовательностей. В данном методе усиления секретности классическая информация перед ее передачей обрабатывается с помощью квантовых перепутанных состояний, используются сгенерированные троичные псевдослучайные последовательности вместо ресурсоемкого генерирования обратимых матриц над полем Галуа $GF(3^2)$, это позволяет повысить скорость в 22,1 – 36,2 раза (для симметрических криптографических систем с длинной (ключа 128-256 бит) без потери стойкости детерминистических протоколов квантовой криптографии с использованием пар кутритов к некогерентной атаке. Это в свою очередь позволяет повысить скорость передачи без потери стойкости детерминистических протоколов квантовой криптографии с использованием пар кутритов к некогерентной атаке;

4. Реализована комбинированная модель на основе разработанных моделей режима контроля подслушивания и режима передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов с использованием метода усиления секретности, что позволило улучшить метод безопасного распределения ключей, повысить скорость и обеспечить помехоустойчивость деполяризационного квантового канала.

Заключительный раздел диссертационной работы будет посвящен имитационному моделированию, а также использованию ПО и аппаратных средств для подтверждения гипотез и результатов, полученных во втором и третьем разделах.

4 ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ РАЗРАБОТАНЫХ МОДЕЛЕЙ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

В предыдущем разделе диссертационной работы были разработаны модели квантового детерминистического протокола в двух базовых режимах работы, в частности их математическое описание и обоснование. В связи с этим, в четвертом разделе работы предлагается провести имитационное моделирование предложенных моделей для получения статистических данных, верификации и подтверждения их преимуществ по сравнению с существующими на сегодняшний день подходами.

4.1 Моделирование квантового детерминистического протокола в режиме контроля подслушивания

Модель имитирует работу детерминистического протокола с парами кутритов в деполяризованном канале при наличии атаки нарушителя Е. В процессе исследования и моделирования работы детерминистического протокола в режиме контроля подслушивания получены статистические данные по уровням ошибок в *x-, z-* базисах и их средние значения. Полученные статистические данные позволяют получить практические рекомендации по возможностям использования детерминистического протокола в квантовом канале с шумом. Кроме того, в данной модели использовался не квантовый способ усиления безопасности детерминистического протокола [52, с.819, 65-68, с.131].

Для начала процесса передачи сообщения пользователь А преобразует свое троичное сообщение *a (a=(a1, …, al), i=1,…, l)* некоторой фиксированной длины $r\cdot$, затем для каждого блока отдельно генерируется случайная троичная последовательность *G(G=(G1, …, Gl), i=1, …, l)*), размером $r\cdot l$, каждый блок которой G_i поразрядно суммируется по модулю 3 с соответствующими блоками сообщения a_i:

$$b_i = a_i + G_i . \tag{4.1}$$

Далее с помощью квантового протокола по квантовому каналу результирующее сообщение *b, (b= (b1, …, bl), i=1, …, l)* передается пользователю Б. В случае перехвата сообщения нарушителем Е, воспользоваться ими он не сможет, так как, не имея случайно сгенерированных последовательностей G_i, он не сможет восстановить исходное сообщение.

После завершения передачи по квантовому каналу, только в том случае, когда обе стороны будут уверены в том, что сеанс передачи не был подслушан нарушителем Е, передаются пользователю Б по классическому открытому каналу случайно сгенерированные последовательности G_i. Для восстановления исходного сообщения пользователь Б должен воспользоваться полученными случайными последовательностями вычитая их из соответствующих блоков сообщения:

$$a_i = b_i\text{-}G_i \tag{4.2}$$

Длина блока *r* подобрана таким образом, чтобы после передачи одного блока можно было добиться высокого уровня устойчивости, а также незначительной вероятности успешной атаки нарушителя Е:

$$s(s(I,q,d)= \left(\frac{1-q}{1-q(1-d)}\right)^{I/I_0} .$$

Длину блока определили по формуле:

$$r = -kI_0 / \lg((1-q)/(1-q\cdot(1-d))) . \tag{4.3}$$

где *k* - показатель степени для расчета вероятности не обнаруженной атаки нарушителя Е; I_0 -количество информации, которое может получить нарушитель Е за один цикл режима передачи сообщения; *q* -вероятность перехода в режим контроля подслушивания; *d* - уровень ошибок, возникающий от действий нарушителя Е [73, с.84].

Для моделирования работы детерминистического протокола с парами кутритов использованы следующие параметры [49, с.7]:

1) длина передаваемых троичных данных – *length =100000* трит;

2) показатель степени десяти для расчета вероятности не обнаруженной атаки нарушителя Е – *k=4*, то есть $s(I,q,d)= 10^{-k}$;

3) вероятности переключения протокола в режим контроля подслушивания и передачи сообщения *q* могут принимать значения от 0,1 до 0,9;

4) чтобы рассчитать значения *r* (4.3) выберем:

$I_0 = 2$ – возможное количество информации, которое может снять нарушитель Е за один раунд передачи, $d = 1/3$ – уровень ошибок, который может возникнуть от действий нарушителя Е в соответствии с работой [72, с.86]);

5) вероятность обнаружения атаки, измеряемой в базисе $x\text{-}d_x=0$ к *2/3*;

6) вероятность обнаружения атаки, измеряемой в базисе $z\text{-}d_z=2/3$;

7) вероятность деполяризации состояния кутрита – *p=0…0,7* и вероятность неизменности состояния кутрита *(1-p)*;

8) вероятность переключения пользователей А и Б между базисами *x*- и *z*- $q_x=q_z=0,5$.

Перед моделированием необходимо задать значения: *length, q,* d_x и *p*, а затем выполнить следующие операции [48, с.11, 49, с.7]:

1. Определение средней вероятности обнаружения атаки по двум базисам в идеальном канале, то есть величина d_{Eva} выражением $d_{Eva} = q_z d_z + q_x d_x$.

Данный параметр определяет средний уровень ошибок, регистрируемый в режиме контроля подслушивания в идеальном канале и нужен для сравнения с

соответствующей величиной в канале с шумом $R_{полна}$ (4.1), учитывающей одновременное изменение состояний передаваемых фотонов в результате действий нарушителя Е и природного шума.

2. Определение длины блока данных r (4.3) и количество этих блоков l, на которое разбиваются передаваемые данные, l определяется выражением $l = length/r$.

3. Определение вероятностей ошибок при измерении в базисах x, z и среднего значения по двум базисам, т.е. параметры Err_x, Err_z, Err_{mean}, выражениями:

$$Err_x = d_x + 3/4 \cdot p \cdot (1 - 3/2 \cdot d_x),$$
$$Err_z = d_z + 3/4 \cdot p \cdot (1 - 3/2 \cdot d_z),$$
$$Err_{mean} = q_x \cdot Err_x + q_z \cdot Err_z. \quad (4.4)$$

4. Генерирование псевдослучайной троичной последовательности a размером $length$ (вероятность генерации состояний «0», «1», «2» бралась равной $1/3$).

5. Разбиение полученной в предыдущем пункте троичной последовательности a, $(a=(a_1, \ldots, a_l), i=1, \ldots, l)$ размером $r \cdot$ на l блоков меньшего объема, при этом последний блок, при необходимости, дополняется случайными тритами, для получения необходимой длины r, затем выполняем над ними операции:

- генерирование случайной последовательности в поле GF(3)

$G(G=(G_1, \ldots, G_l), i=1, \ldots, l)$ размером $r \cdot l$.

- сложение $a_i + G_i$ в поле Галуа GF(3), в результате получили b_i (4.2).

- передача b_i с помощью детерминистического протокола в квантовом канале с шумом.

Переключение между режимами контроля подслушивания и передачи сообщения происходит с вероятностями q и $(1-q)$. В режиме передачи сообщения по квантовому каналу пользователь Б получает пару кутритов, причем ошибки проявляются из-за воздействия как атаки нарушителя Е, так и естественного шума канала, ошибки не моделировались. С равными вероятностями $q_x = q_z = 1/2$ в режиме контроля подслушивания выбирается определенный базис и подсчитывается общее число переходов в определенный базис (Kp_x, Kp_z). Далее моделируется ошибка либо для базиса x с вероятностью Err_x, либо для базиса z с вероятностью Err_z, далее подсчитывается количество ошибок Co_{Dx} и Co_{Dz}. Процесс переключения между режимами повторяется до тех пор, пока не будет полностью передан блок b_i.

Далее после того как получены все блоки b_i пользователь А передает Б открытым каналом $G(G_1, \ldots, G_l), i=1, \ldots, l)$, после чего мы получим a_i: $a_i = b_i - g_i$.

- рассчитываем средний уровень ошибок в базисах x, z и средний уровень ошибок для двух базисов по каждому переданному блоку b_i: $b_i\_Errlvl_x$, $b_i\_Errlvl_z$ и $b_i\_Errlvl_{mean}$ выражениями:

$$b_i\_Errlvl_x = Co_{Dx}/Kp_x\ ;\ b_i\_Errlvl_z = Co_{Dz}/Kp_z\ ,$$
$$b_i\_Errlvl_{mean} = (Co_{Dx} + Co_{Dz})/(Kp_x + Kp_z)\ . \qquad (4.5)$$

6. По полученным значениям проведен расчет минимальных ($MinErrlvl_x$, $MinErrlvl_z$, $MinErrlvl$) и максимальных ($MaxErrlvl_x$, $MaxErrlvl_z$, $MaxErrlvl$) значений уровней ошибок, средние значения ($MeanErrlvl_x$, $MeanErrlvl_z$, $MeanErrlvl$) по всем l переданных блоков.

На рисунках 4.1 – 4.2 представлены результаты вероятностей деполяризации состояния кутрита при моделировании работы протокола при различных значениях q, D_x, D_z, D_{eva}.

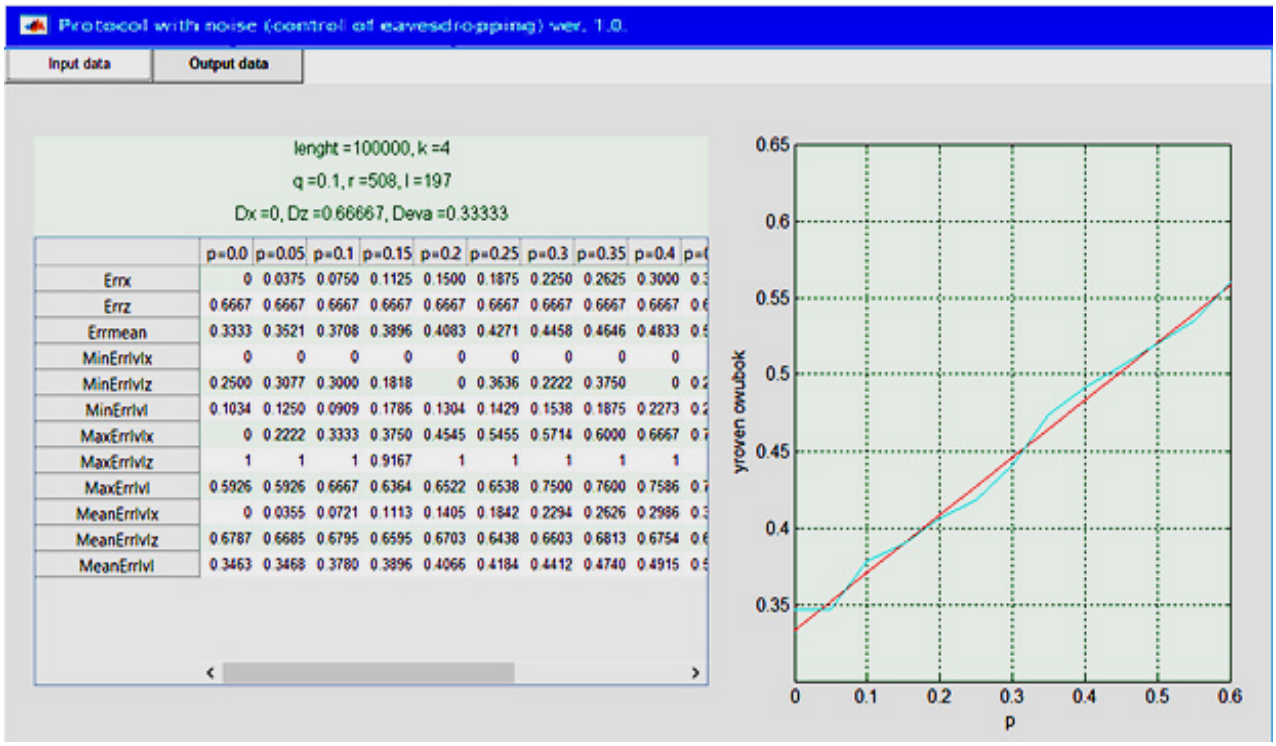


Рисунок 4.1 – Значения уровней ошибок при моделировании с $q=0,1$; $D_x=0$; $D_s=0,6667$; $D_{eva}=0,3333$ и вероятностей деполяризации состояния кутрита от $p=0,0$ до $p=0,4$

В таблицу 4.1 сведены все результаты моделирования.

1. По результатам мы видим, что в пределах статистической погрешности полученные средние значения уровня ошибок по всем переданным блокам *MeanErrlvl* равны соответствующим теоретическим значениям *Errmean*. Однако это возможно только в случае передачи достаточно большого объема передаваемых блоков данных. Но в тоже время, минимальные уровни ошибок по обоим базисам (*MeanErrlvl*) достаточно малы и в большинстве случаев меньше уровня естественного шума p, особенно при больших p (таблица 4.1). Все это является следс-

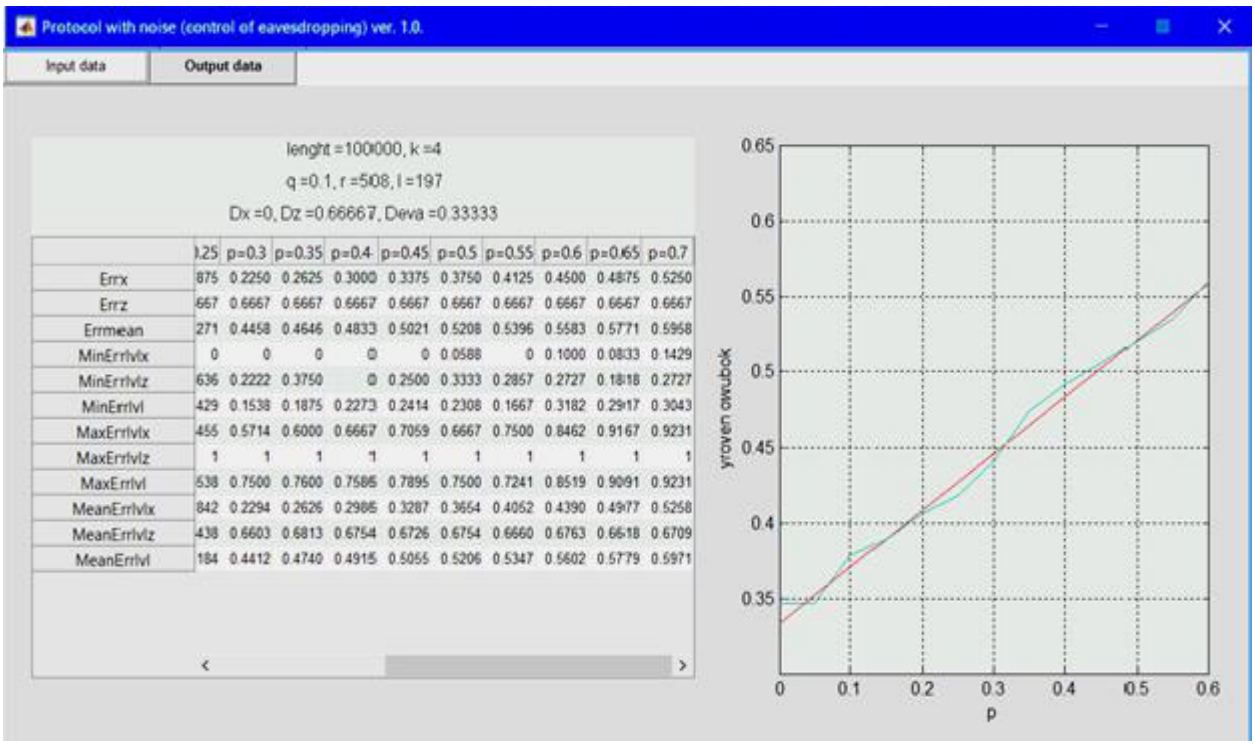


Рисунок 4.2 – Значения уровней ошибок при моделировании с $q=0,1$; $D_x=0$; $Dz=0,6667$; $D_{eva}=0,3333$ и вероятностей деполяризации состояния кутрита от $p=0,3$ до $p=0,7$

твием случайной природы квантовых измерений. Таким образом, передав один блок и проверив уровень ошибок в режиме контроля подслушивания, Пользователи А и Б могут сделать ошибочный вывод, что подслушивания нет. Поэтому в шумном канале, в частности при достаточно высоком уровне естественных шумов, легитимные пользователи должны передать достаточно большое количество блоков, как минимум несколько десятков, и только после этого принять решение либо о наличии, либо об отсутствии атаки нарушителя Е (и соответственно о необходимости, либо прерывания работы протокола, либо передачи псевдослучайной последовательности G от пользователя А к пользователю Б).

Все это является основой для выработки рекомендаций по практической реализации детерминистического протокола с перепутанными парами кутритов в деполяризованном канале.

2. Средние уровни ошибок почти не зависят от вероятности переключения в режим контроля подслушивания q (таблица 4.1).

Но эта вероятность существенно влияет на скорость передачи данных детерминистическим протоколом: чем меньше q, тем чаще передаются данные и тем выше скорость. Но от q также зависит и длина блока r, с уменьшением q согласно экспоненциального закона она увеличивается [48, с. 12].

3. При $p=0,7$ и атаке нарушителя Е с нулевым уровнем ошибок в одном из базисов (например, $d_x=0$, $d_{Eva}=0,333$), средний уровень ошибок *MeanErrlvl* почти не превышает p, поэтому легитимные пользователи могут принять неверное решение об отсутствии атаки. Поэтому необходимо проверить средний уровень

Таблица 4.1 – Результаты моделирования режима контроля подслушивания

d			d_x=0; d_z=0,667; d_{Eva}=0,333				d_x=0,333; d_z=0,667; d_{Eva}=0,5				d_x=0,667; d_z=0,667 ; d_{Eva}=0,667			
p			**p=0,1**	**p=0,3**	**p=0,5**	**p=0,7**	**p=0,1**	**p=0,3**	**p=0,5**	**p=0,7**	**p=0,1**	**p=0,3**	**p=0,5**	**p=0,7**
Errx			0,075	0,225	0,375	0,525	0,371	0,446	0,521	0,596	0,667	0,667	0,667	0,667
Errz			0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667
Errmean			0,371	0,446	0,521	0,596	0,519	0,556	0,594	0,631	0,667	0,667	0,667	0,667
k=4;length=100000	q=0,5;r=66;l=1516	MinErrlvlx	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,143	0,286	0,143	0,250	0,200
		MinErrlvlz	0,167	0,143	0,300	0,200	0,167	0,143	0,200	0,286	0,000	0,167	0,273	0,154
		MinErrlvl	**0,080**	**0,154**	**0,240**	**0,296**	**0,120**	**0,267**	**0,280**	**0,273**	**0,381**	**0,370**	**0,353**	**0,320**
		MaxErrlvlx	0,375	0,600	0,875	1	1	0,909	1	1	1	1	1	1
		MaxErrlvlz	1	1	1	1	1	1	1	1	1	1	1	1
		MaxErrlvl	0,655	0,809	0,794	1	0,857	0,920	0,833	0,875	0,960	0,929	0,952	0,949
		MeanErrlvlx	0,075	0,224	0,378	0,521	0,372	0,444	0,519	0,594	0,668	0,666	0,664	0,667
		MeanErrlvlz	0,663	0,666	0,665	0,670	0,661	0,666	0,663	0,665	0,665	0,667	0,673	0,666
		MeanErrlvl	**0,369**	**0,445**	**0,522**	**0,596**	**0,517**	**0,554**	**0,591**	**0,630**	**0,666**	**0,666**	**0,668**	**0,667**
	q=0,25;r=176;l=569	MinErrlvlx	0,000	0,000	0,000	0,100	0,000	0,000	0,143	0,125	0,120	0,333	0,200	0,273
		MinErrlvlz	0,308	0,333	0,200	0,200	0,286	0,200	0,273	0,200	0,200	0,273	0,231	0,111
		MinErrlvl	**0,115**	**0,167**	**0,200**	**0,360**	**0,263**	**0,290**	**0,320**	**0,343**	**0,385**	**0,333**	**0,381**	**0,375**
		MaxErrlvlx	0,375	0,667	0,800	0,933	0,875	0,846	0,857	0,929	1	1	1	1
		MaxErrlvlz	1	1	1	1	1	1	1	1	1	1	1	1
		MaxErrlvl	0,654	0,711	0,793	0,936	0,905	0,813	0,852	0,905	0,917	0,909	0,931	0,931
		MeanErrlvlx	0,076	0,225	0,376	0,536	0,363	0,451	0,535	0,598	0,667	0,664	0,669	0,667
		MeanErrlvlz	0,677	0,660	0,664	0,665	0,665	0,657	0,666	0,666	0,663	0,663	0,666	0,668
		MeanErrlvl	**0,374**	**0,441**	**0,518**	**0,599**	**0,516**	**0,556**	**0,601**	**0,632**	**0,666**	**0,663**	**0,667**	**0,668**
	q=0,1;r=508;l=197*q*=0,1;*r*=508;*l*=1	MinErrlvlx	0,000	0,000	0,059	0,143	0,083	0,000	0,000	0,250	0,333	0,211	0,300	0,273
		MinErrlvlz	0,300	0,222	0,333	0,273	0,200	0,273	0,333	0,286	0,200	0,308	0,375	0,333
		MinErrlvl	**0,091**	**0,154**	**0,231**	**0,304**	**0,226**	**0,227**	**0,318**	**0,353**	**0,382**	**0,367**	**0,423**	**0,419**
		MaxErrlvlx	0,333	0,571	0,667	0,923	0,779	1	0,917	0,889	1	1	1	1
		MaxErrlvlz	1	1	1	1	0,933	1	1	1	1	0,947	1	1
		MaxErrlvl	0,667	0,750	0,750	0,923	0,800	0,828	0,833	0,900	0,944	0,929	0,947	0,909
		MeanErrlvlx	0,072	0,229	0,365	0,526	0,375	0,454	0,508	0,589	0,673	0,653	0,672	0,662
		MeanErrlvlz	0,679	0,660	0,675	0,671	0,651	0,657	0,677	0,669	0,677	0,653	0,679	0,664
		MeanErrlvl	**0,378**	**0,441**	**0,521**	**0,597**	**0,514**	**0,556**	**0,593**	**0,629**	**0,671**	**0,655**	**0,675**	**0,662**

ошибок в каждом из базисов x и z отдельно, в одном из этих базисов уровень ошибок будет близок к значению $2/3$. Кроме того, можно сделать вывод: для надежного детектирования атаки легитимные пользователи должны использовать квантовый канал с естественным уровнем шумов, на практике это означает использование канала ограниченной длины.

Анализ статистических данных экспериментального исследования предложенной имитационной модели проведен на основе полученных данных (таблица 4.1). На рисунках 4.3-4.5 представлены диаграммы зависимостей *min* значения уровней ошибок, *MinErrlvl* при моделировании работы детерминистического протокола при различных значениях d_x, d_z, d_{Eva}, которые построены на основе таблиц 4.2-4.4 [49, с.8].

Таблица 4.2 – Результаты моделирования для d_x=0, d_z=0,667, d_{Eva}=0,333

Q	p1	p2	p3	p4
0,1	0,091	0,154	0,231	0,304
0,25	0,115	0,167	0,2	0,36
0,5	0,08	0,154	0,24	0,296

Таблица 4.3 – Результаты моделирования для d_x=0,333, d_z=0,667, d_{Eva}=0,5

Q	p1	p2	p3	p4
0,1	0,226	0,227	0,318	0,353
0,25	0,263	0,29	0,32	0,343
0,5	0,263	0,29	0,32	0,343

Таблица 4.4 – Результаты моделирования для d_x=0,667, d_z=0,667, d_{Eva}=0,5

Q	p1	p2	p3	p4
0,1	0,382	0,367	0,423	0,419
0,25	0,385	0,333	0,381	0,375
0,5	0,381	0,37	0,353	0,32

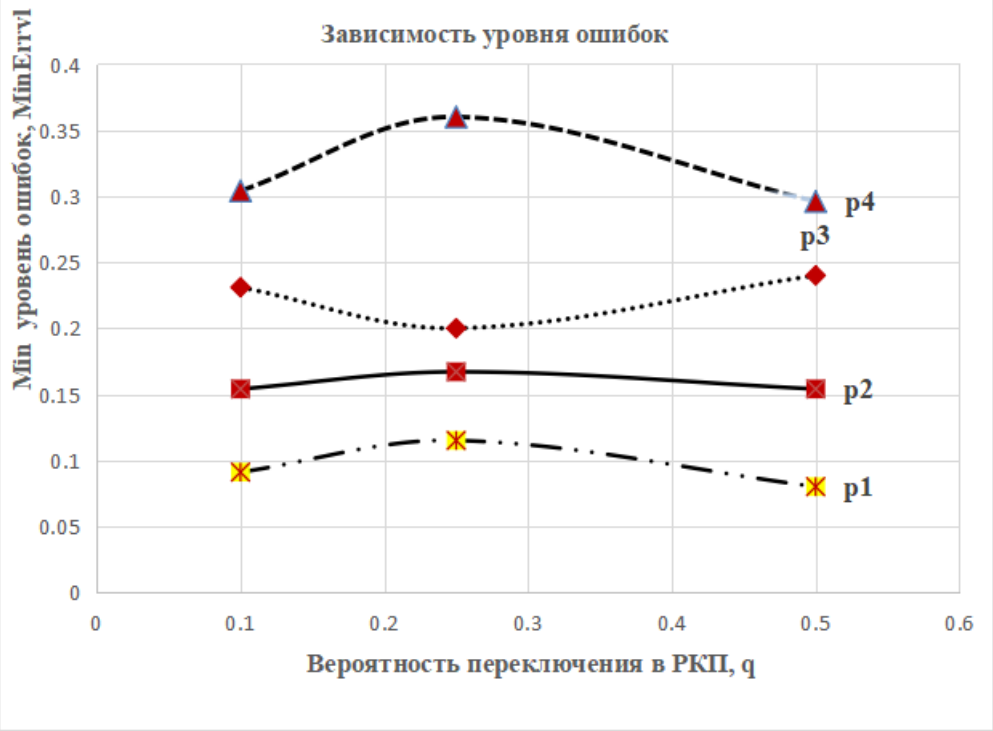


Рисунок 4.3 – Зависимость *min* значения уровней ошибок, *MinErrlvl* при моделировании $d_x=0$, $d_z=0,667$, $d_{Eva}=0,333$ и вероятностей деполяризации состояния кутрита от $p=0,1$ до $p=0,7$

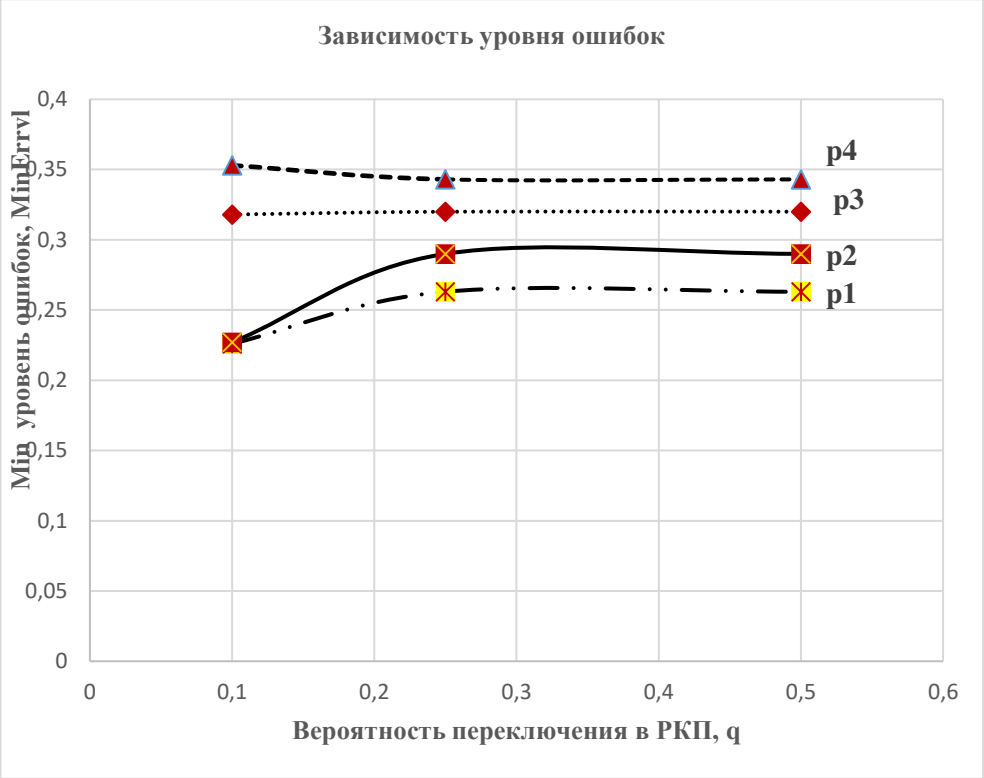


Рисунок 4.4 – Зависимость *min* значения уровней ошибок, *MinErrlvl* при моделировании $d_x=0,333$, $d_z=0,667$, $d_{Eva}=0,5$ и вероятностей деполяризации состояния кутрита от $p=0,1$ до $p=0,7$

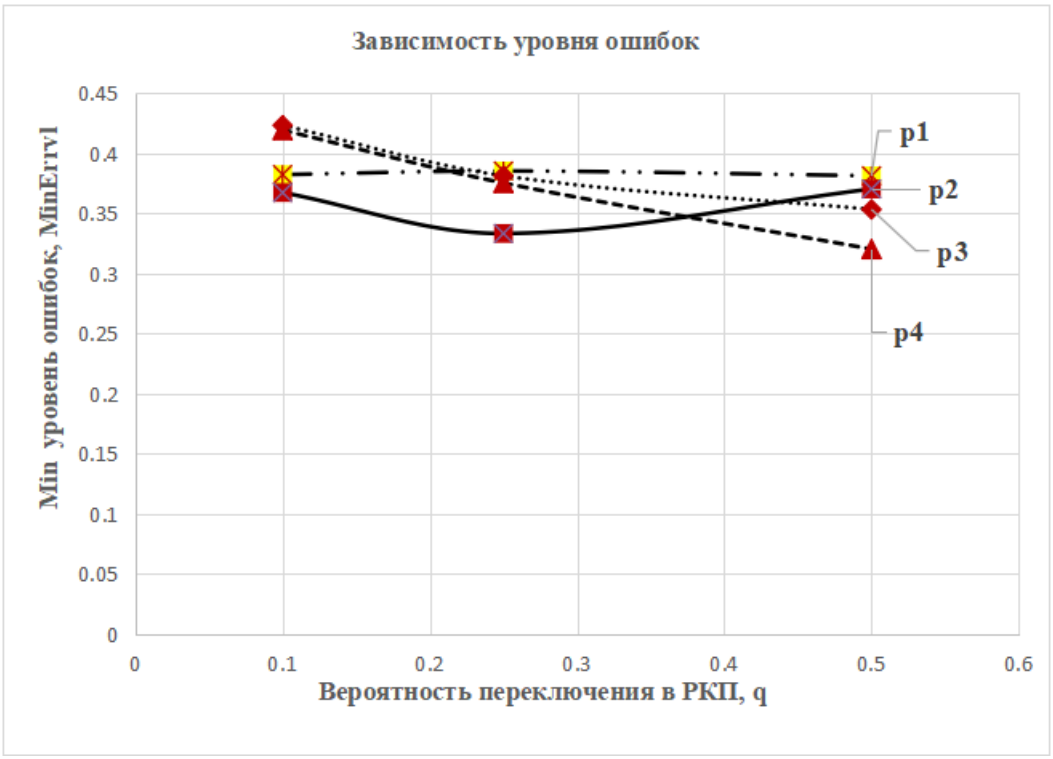


Рисунок 4.5 – Зависимость *min* значения уровней ошибок, *MinErrlvl* при моделировании $d_x=0,667$, $d_z=0,667$, $d_{Eva}=0,667$ и вероятностей деполяризации состояния кутрита от от $p=0,1$ до $p=0,7$

Проведя анализ данных рисунков 4.3-4.5, можно сделать следующие выводы [49, с.9]:

1. Минимальные уровни ошибок по обоим базисам (*MinErrlvl)* достаточно малы и в большинстве случаев меньше уровня естественного шума p (особенно при $p \rightarrow 0,7$). Это означает, что пользователи А и Б могут сделать ошибочный вывод касательно присутствия нарушителя Е, поэтому при достаточно высоком уровне естественных шумов, легитимные пользователи должны передать достаточно большое количество блоков и только после этого принять решение о наличии или отсутствии атаки нарушителя Е;

2. Вероятность q существенно влияет на скорость передачи данных детерминистическим протоколом – так, чем меньше q, тем чаще передаются данные и тем выше скорость. Кроме этого, от q также зависит и длина блока r – с уменьшением q согласно экспоненциального закона она увеличивается;

3. При $p \rightarrow 0,7$ и атаке нарушителя Е с нулевым уровнем ошибок в одном из базисов (например, $d_x=0$, $d_{Eva}=0,333$), средний уровень ошибок *MeanErrlvl* почти не превышает p, поэтому легитимные пользователи могут принять неверное решение об отсутствии атаки – необходимо проверить средний уровень ошибок в каждом из базисов x и z отдельно, в одном из этих базисов уровень ошибок будет близок к значению $2/3$;

4. Для надежного детектирования атаки легитимные пользователи должны использовать квантовый канал с естественным уровнем шумов – на практике это означает использование канала ограниченной длины.

Таким образом, разработана модель детерминистического протокола в режиме контроля подслушивания с парами кутритов в канале с шумом и промоделирована ее работа в канале с шумом. Получена формула полной вероятности ошибочного результата при измерении в режиме контроля подслушивания. Обоснована равность величин максимальной вероятности ошибки в режиме контроля подслушивания при реализации протокола в идеальном и шумном деполяризованном каналах. Установлено, что в деполяризованном канале, особенно при достаточно высоком уровне шумов, легитимные пользователи должны передать достаточно большое количество блоков информации (как минимум несколько десятков) и только после этого принять решение либо о наличии, либо об отсутствии атаки. Также установлено, что легитимные пользователи для надежного детектирования атаки на практике должны использовать квантовый канал ограниченной длины с естественным уровнем шумов $p \leq 0,7$. Данная модель в дальнейшем может быть усовершенствована, добавлением механизма для учета ошибок в режиме передачи сообщения и использованием помехоустойчивого кодирования для кутритов [49, с.8].

4.2 Моделирование квантового детерминистического протокола в режиме передачи сообщений

Для моделирования работы детерминистического протокола с парами кутритов и применением РС-кодов использованы входные параметры [55, с. 154]:

1) *length =100000* трит - длина передаваемых троичных данных;

2) *k=4* (фиксированный необходимый уровень безопасности);

3) *q=0,5* – вероятность переключения протокола в режим контроля подслушивания и (*1-q)* – вероятность переключения в режим передачи сообщений (данная стратегия переключения между режимами считается [17, с.3] наиболее оптимальной для субъектов А и Б);

4) Для расчета величины *r* выбрано: $I_0=2$ – количество информации, которую может получить субъект Е за один раунд (предположив, что субъект Е может получить 2 трита), *d=1/3* - уровень ошибок, предположительно создаваемый субъектом Е (минимально возможный уровень ошибок см. [63, с.46]);

5) *p=0, …, 0,5* - уровень (вероятность) деполяризации (перебор с шагом 0,01).

Параметр ρ фиксирован, далее выполнялись операции [49, с.8]:

Первый шаг. С учетом необходимого уровня безопасности, рассчитывается длина блока данных *r* [63, с.51] и количество этих блоков *l*, на которые разбивались передаваемые данные. Для удобства применения РС-кодов *r* выбрано кратным 8, а величина *l* рассчитывается по формуле *l=length/r*.

Второй шаг. Генерирование троичных ПСЧП длиной *length*. Для генерирования ПСЧП использован предложенный авторами в [71, с.143] алгоритм TriGen, на основе метода генерирования тритовых ПСЧП ξ (псевдокод алгоритма на рисунке 4.6). В алгоритме TriGen используются такие параметры:

d=4; s=6; l=ds=24; p=l 14=336; n=4l= 96; e=p-n=10 l=240; m=b n=96b; r=4; b - натуральное число. Операция *Sbox(X)* выполняет нелинейную замену каждые шесть тритов числа *X* на соответствующие им значения таблицы подстановок. Используемая таблица подстановок, построена с помощью расчета обратного элемента поля $(X)^{-1} \in GF(3^6)$ с последующим выполнением аффинного преобразования над полем $GF(3): S(X)=M(X)^{-1}+V$, где $X,V \in GF(3^6)$, а *M* - квадратная не вырожденная матрица над полем *GF(3)* размером 6×6. Конечное поле $GF(3^6)$ фиксируется кольцом многочленов с операциями по модулю неприводимого многочлена $m(x) = x^6+x+2$ [71, с. 144].

Таблица замен построена на таких значениях матрицы *M'* и вектора *V*:

$$M = \begin{pmatrix} 1 & 2 & 01 & 2 & 2 \\ 2 & 1 & 20 & 1 & 1 \\ 1 & 2 & 10 & 1 & 1 \\ 1 & 0 & 21 & 2 & 0 \\ 0 & 1 & 02 & 1 & 2 \\ 2 & 0 & 11 & 2 & 1 \end{pmatrix}; V = \begin{pmatrix} 0 \\ 2 \\ 2 \\ 1 \\ 0 \\ 2 \end{pmatrix}.$$

Операция *Mix(X)* выполняется умножением квадратной не вырожденной матрицы тритов *M'* размером 24×24 над полем *GF(3)* на вектор-столбец *X* над полем *GF(3)*. Матрица *M'* построена на основе массива *U* следующим образом:

M'[i][j]=U[(j+24-i)mod 24], где $i,j = \overline{1, \ldots, 23}$, а массив *U* принимает значения:

U={1, 0, 2, 2, 1, 0, 2, 0, 1, 1, 1, 2, 0, 1, 2, 1, 0, 2, 0, 0, 1, 2, 0, 2}.

*Третий шаг***.** Сгенерированные на предыдущем шаге ПСЧП разбиваются на l меньших блоков $a_i (i = 1, \ldots, l)$ размером r (последний блок при необходимости дополняется до размера r случайными тритами), над ними выполняются операции:

1. Для каждого блока генерируется случайная последовательность G_i над полем $GF(3)$ размером r на l.

2. Выполняется сложение a_i со случайной последовательностью G_i в поле Галуа $GF(3)$, в результате получили b_i: $b_i = a_i + G_i$.

3. Далее результат разбивается на под блоки по 8 тритов и с помощью РС-кодов кодируются, в результате каждый под блок увеличивается в длину до 16 тритов, затем под блоки снова объединяются и получается блок размером $2r$.

4. С помощью детерминистического протокола по квантовому каналу с шумом выполняется передача. С вероятностями q и $(1-q)$ происходит переключение между двумя режимами протокола. Это переключение происходит до тех пор, пока полностью не будет передан весь блок.

TriGen v.2.0

Input: вектор инициализации VI, секретный ключ K, $VI \in V_{240}$, $K \in V_{96}$, параметр b.

Output: выходная последовательность $M = (M_1, \ldots, M_b)$, $M \in V_{96b}$, $M_q \in V_{96}$, $q \in \overline{1,b}$.

1. $x_i = VI_i$, $y_j = VI_{6+j}$, $k_j = K_j$, $i \in \overline{1,6}$, $j \in \overline{1,4}$.

2. $For\ q = 1; q \le b;\ q{+}{+}\ do$

2.1. $For\ j = 0;\ j < 4;\ j{+}{+}\ do$

2.1.1. $x_1 = \left(Sbox\left(x_1 + k_1\right) \oplus x_4\right) <<< k_4$; $x_2 = \left(Sbox\left(x_2 + k_2\right) + x_5\right) >>> k_3$; $x_3 = Mix\left(\left(x_3 + x_6\right) \oplus y_3\right) <<< x_1$;

2.1.2. $k_1 = Sbox\left(\left(Sbox\left(x_1 \oplus k_1\right) + x_5\right) \oplus y_1\right)$; $k_2 = Sbox\left(Mix\left(x_2 + k_2 + x_6\right) \oplus y_2\right)$;

2.1.3. $y_1 = Sbox\left(\left(\left(k_1 + y_1\right) <<< x_2\right) \oplus k_3\right)$; $y_2 = Mix\left(Sbox\left(\left(\left(k_2 + y_2\right) >>> x_3\right) \oplus k_4\right)\right)$;

2.1.4. $x_4 = \left(Sbox\left(x_4 + k_3\right) \oplus x_1\right) <<< k_2$; $x_5 = \left(Sbox\left(x_5 + k_4\right) + x_2\right) >>> k_1$; $x_6 = Mix\left(\left(x_6 + x_3\right) \oplus y_1\right) <<< x_4$;

2.1.5. $k_3 = Sbox\left(\left(Sbox\left(x_4 \oplus k_3\right) + x_2\right) \oplus y_3\right)$; $k_4 = Sbox\left(Mix\left(x_5 + k_4 + x_3\right) \oplus y_4\right)$;

2.1.6. $y_3 = Sbox\left(\left(\left(k_3 + y_3\right) <<< x_5\right) \oplus k_1\right)$; $y_4 = Mix\left(Sbox\left(\left(\left(k_4 + y_4\right) >>> x_6\right) \oplus k_2\right)\right)$.

2.2. $M_q = \left(y_1 \mid y_2 \mid y_3 \mid y_4\right)$

Рисунок 4.6 – Псевдокод алгоритма TriGen [71, с.144 , 74-76]

Моделирование режима контроля подслушивания выполнено в работе [51, с.62]. В режиме передачи сообщения моделируется поочередный прием субъектом Б каждой пары тритов блока b_{k_i} через квантовый канал (ошибки, здесь обусловлены только шумом в канале, предположив, что субъект Е не выполняет подслушивания). Каждые 8 пар принятых тритов блока b_{k_i} пытались расшифровать с помощью РС-кодов.

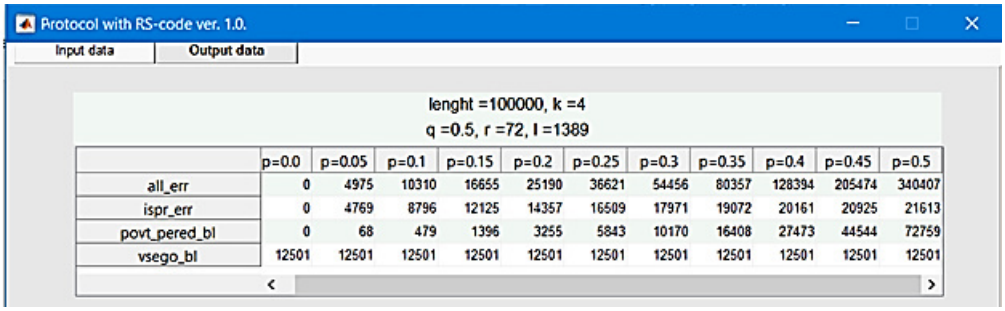
Если количество искаженных шумом пар тритов было меньше трех, коды их безошибочно исправляли, в противном случае эти 8 пар тритов передавали

повторно (используется так называемое корректирующее кодирование с обратной связью). В результате декодирования РС-кодами с b_{k_i} получали b_i размером r. При моделировании ошибок в канале с шумом учитывалась симметрия деполяризующего канала (ДПК), а именно $p/8$ вероятность замены соответствующей пары тритов на одну из 8-ми других. Следующий шаг восстановление исходного сообщения a_i, для этого выполнялось вычитание в поле Галуа GF(3). Для каждого переданного блока b_k рассчитывались $bk_i\_all\_err$, $bk_i\_ispr\_err$, $bk_i\_povt\_blok$ (количество ошибок, количество исправленных ошибок и количество раз повторной передачи данного подблока).

Четвертый шаг. На основе собранной статистики по каждому b_{k_i} рассчитывались общие показатели *all_err, ispr_err* и *povt_blok*, которые необходимы для оценки уровня доступности системы КПБС в ДПК с использованием предложенных РС-кодов.

Обработка результатов моделирования

С целью проведения статистического моделирования работы режима передачи сообщений (с применением РС-кодов для кутритов и метода усиления секретности) в среде MATLAB было разработано соответствующее программное обеспечение (см. рисунок 4.7) [55, с.156].



	p=0.0	p=0.05	p=0.1	p=0.15	p=0.2	p=0.25	p=0.3	p=0.35	p=0.4	p=0.45	p=0.5
all_err	0	4975	10310	16655	25190	36621	54456	80357	128394	205474	340407
ispr_err	0	4769	8796	12125	14357	16509	17971	19072	20161	20925	21613
povt_pered_bl	0	68	479	1396	3255	5843	10170	16408	27473	44544	72759
vsego_bl	12501	12501	12501	12501	12501	12501	12501	12501	12501	12501	12501

Рисунок 4.7 – Результат моделирования работы детерминистического протокола в режиме передачи сообщений

В результате моделирования получены статистические данные, на основе которых построены графики (см. рисунки 4.8-4.9), подтверждающие пригодность данных кодов для коррекции ошибок при реализации типовых протоколов КПБС в ДПК. В частности, полученная статистическая информация показывает, что коды хорошо справляются с коррекцией ошибок, если вероятность деполяризации кутритов p в квантовом канале не превышает 25%при этом количество повторно переданных подблоков составляет 47% от их общего количества. При *p=10%* количество повторно переданных подблоков составляет всего 3,8% от их общего количества. Поскольку в современных экспериментах уровень ошибок при передаче фотонов квантовым каналом, как правило, не превышает нескольких процентов, то можно сделать вывод, что троичные РС-коды вполне пригодны для корректирующего кодирования в типичных протоколах КПБС с передачей кутритов.

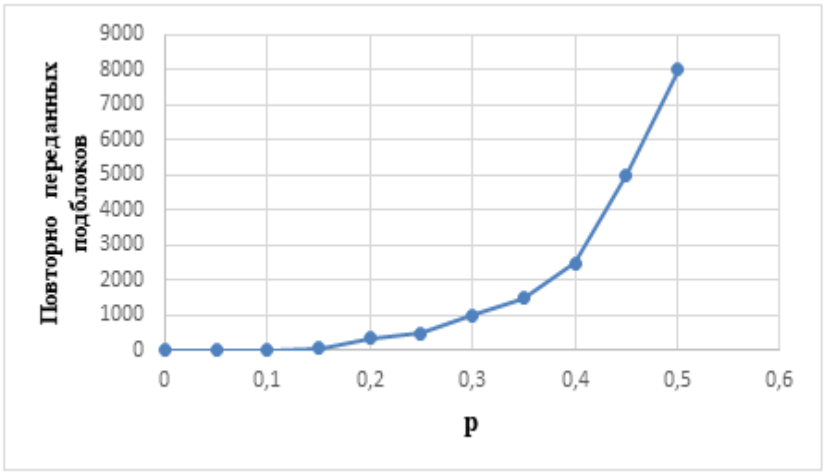


Рисунок 4.8 – Зависимость количества полученных и исправленных ошибок от деполяризации *p*

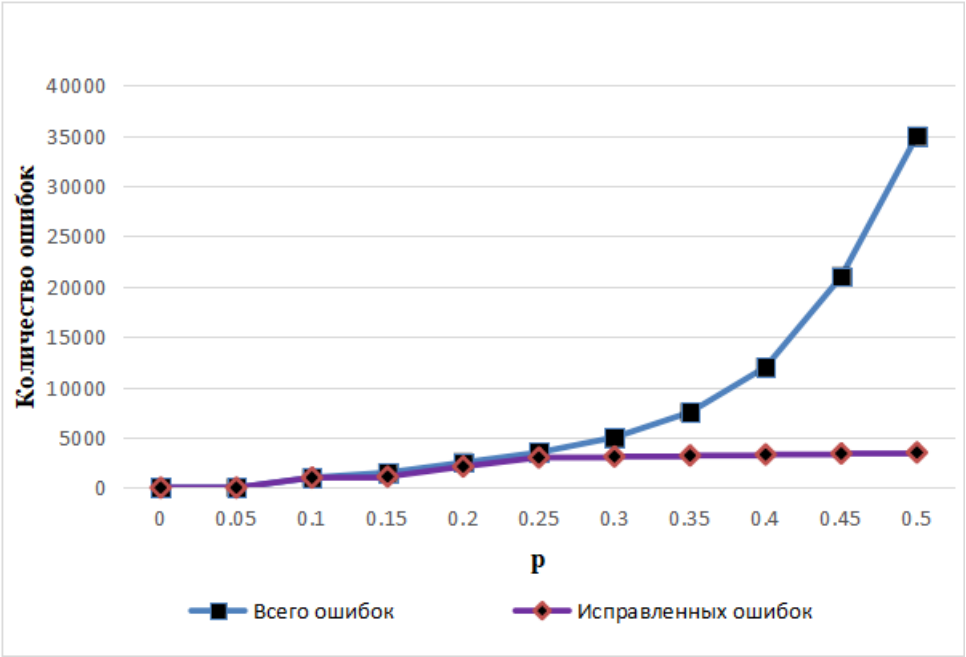


Рисунок 4.9 –Зависимость от деполяризации *p* количества полученных и исправленных ошибок, а также количества повторно переданных подблоков

Однако, указанное процентное ограничение не является критическим и может меняться разработчиками квантовых систем безопасности в зависимости от условий эксплуатации, ожидаемого уровня безопасности, временных ограничений и других факторов. Поэтому, полученные результаты могут служить весомым инструментальным средством эксперта в сфере информационной безопасности при построении эффективных систем КРК и КПБС [19, 77-85].

Экспериментальное исследование корректирующей способности помехоустойчивых кодов Рида-Соломона

Использование детерминистических протоколов с парами перепутанных кутритов позволяет увеличить информационную емкость, и как следствие, скорость передачи информации. Обеспечение ее безошибочной передачи такими протоколами поэтому является актуальной задачей. Данную задачу можно решить с помощью разработки системы троичных РС-кодов. Но троичные коды практически недостаточно полно исследованы и не представлены в открытых источниках, поэтому существует необходимость их детального рассмотрения с целью изучения и испытания их корректирующей способности. Целью эксперимента является оценка корректирующей способности троичных РС-кодов при передаче информации с использованием перепутанных пар кутритов в квантовом канале с шумом.

Описание системы кодов Рида-Соломона над полем Галуа GF (3^2)

РС-коды являются частным случаем кода БЧХ, определения порождающих полиномов, которые лежат в том же поле, над которым и строится код. Для наглядности опишем РС-коды в общем виде. Пусть *a* - элемент поля GF *(q^m)* порядка *n* , где *q,m* - целые числа, причем q>1, m>0, и $q^m \neq 2$. Если *a*- примитивный элемент, то его порядок равен *(q^m-1)*, то есть $a^{q^m-1} = 1$ и $a^i \neq 1$ где *0<i<(q^m-1).* Тогда нормированный полином $g(x)$ минимальной степени над полем GF *(q^m)* решениями которого является *(d-1)* степеней a^{i_0}, $a^{i_0+1}, \ldots, a^{i_0+d-2}$ ..., элемент *a*, является порождающим полиномом РС-кодов над полем *GF(q^m)*, где i_0 - некоторое целое число, с помощью которого иногда удается упростить процедуру кодирования. Обычно $i_0=1$. Степень многочлена $g(x)$ равна *(d-1)*.

Длина полученного кода символов $n = q^m - 1$ и содержит $r = d - 1 = \deg(g(x))$ проверочных символов, где *deg()* означает степень полинома, а – *d* минимальное кодовое расстояние (минимальное из всех расстояний Хемминга для всех пар кодовых символов). Число информационных символов $k = n - r = n - d + 1$. Таким образом, $d = n - k + 1$, коды с подобным значением минимального кодового расстояния в теории кодирования получили название максимальных . РС-коды исправляют $t = r/2$ ошибки, но требуют $r = 2t$ проверочных символов. С их помощью исправляются произвольные пачки ошибок длиной не более чем *t*. Согласно теореме о границе Рейгера [51, с.61], РС-коды являются оптимальными с точки зрения соотношения длины пакета и возможности исправления ошибок.

Процедуры кодирования/декодирования в системе РС-кодов над полем Галуа GF (3^2) формализованы в [51, с.63]. Поскольку при передаче информации квантовым каналом вероятность возникновения ошибок достаточно велика, в данной работе исследуется корректирующая способность РС-кодов над полем Галуа GF (3^2), в которых $k = r$, что позволяет исправлять $t = n/4$ пар ложных тритов. Итак, в работе используются следующие параметры: длина полученного кода $n = q^m - 1 = 3^2 - 1 = 9 - 1 = 8$ пар тритов, минимальное кодовое расстояние $d = 5$, проверочных символов $r = d - 1 = 5 - 1 = 4$ пары тритов, число информационных символов $k = n - r = 8 - 4 = 4$ пары тритов, количество ошибок которые удастся ис-

править $t = r/2 = 2$ пары тритов. Для нахождения порождающего многочлена сначала необходимо описать операции сложения и умножения в поле Галуа GF (3^2). Конечное поле GF (3^2) может быть построено над такими полиномами x^2+1, x^2+x+2, x^2+2x+2, $2x^2+2$, $2x^2+x+1$, $2x^2+2x+1$. В данном эксперименте для построения поля Галуа GF (3^2) использован примитивный полином x^2+x+2. Обозначим все возможные пары тритов, как показано в таблице 4.5 в полиномиальном виде. Тогда, если обозначить x как примитивный элемент a, можно легко посчитать любую троичную пару в виде степени a. Для этого необходимо перемножить известные полиномиальные обозначения степеней a по модулю x^2+x+2, результат показан в таблице 4.5.

На основе таблицы 4.5 построены таблицы сложения и умножения над примитивным полиномом в поле Галуа GF (3^2) (таблица 4.6, таблица 4.7), результаты операций вычитания и деления также можно легко получить из тех же таблиц.

Таблица 4.5 - Элементы поля Галуа GF (3^2) над полиномом

В троичном виде	В виде полинома	В виде степени
1	2	3
00	0	0
01	1	a^8=1
02	2	a^4=2
10	x	a^1
11	x+1	a^7
12	x+2	a^6
20	2x	a^5
21	2x+1	a^2
22	2x+2	a^3

Таблица 4.6 - Сложение в поле Галуа GF (3^2) над полиномом x^2+x+2

+	0	a^8=1	a^4=2	a^1	a^7	a^6	a^5	a^2	a^3
0	0	a^8=1	a^4=2	a^1	a^7	a^6	a^5	a^2	a^3
$\boldsymbol{a^8}$**=1**	a^8=1	a^4=2	0	a^7	a^6	a^1	a^2	a^3	a^5
$\boldsymbol{a^4}$**=2**	a^4=2	0	a^8=1	a^6	a^1	a^7	a^3	a^5	a^2
$\boldsymbol{a^1}$	a^1	a^7	a^6	a^5	a^2	a^3	0	a^8=1	a^4=2
$\boldsymbol{a^7}$	a^7	a^6	a^1	a^2	a^3	a^5	a^8=1	a^4=2	0
$\boldsymbol{a^6}$	a^6	a^1	a^7	a^3	a^5	a^2	a^4=2	0	a^8=1
$\boldsymbol{a^5}$	a^5	a^2	a^3	0	a^8=1	a^4=2	a^1	a^7	a^6
$\boldsymbol{a^2}$	a^2	a^3	a^5	a^8=1	a^4=2	0	a^7	a^6	a^1
$\boldsymbol{a^3}$	a^3	a^5	a^2	a^4=2	0	a^8=1	a^6	a^1	a^7

Для расчета порождающего полинома взят $i_0 = 1$, использовано выражение $g(x) = (x - a^{i_0})(x - a^{i_0+1})...(x - a^{i_0+d-2})$ и таблицы 4.5, таблицы 4.6, таблицы 4.7:

$$g(x) = (x - a^1)(x - a^2)(x - a^3)(x - a^4) = x^4 + a^7x^3 + a^2x^2 + a^4x + a^2 = \overline{a^8a^7a^2a^4a^2}.$$

Зная *g(x), n, k, r* - РС-коды можно применять на практике.

Таблица 4.7 - Умножение в поле Галуа GF (3^2) над полиномом x^2+x+2

*	0	$a^8=1$	$a^4=2$	a^1	a^7	a^6	a^5	a^2	a^3
0	0	0	0	0	0	0	0	0	0
$\boldsymbol{a^8=1}$	0	$a^8=1$	$a^4=2$	a^1	a^7	a^6	a^5	a^2	a^3
$\boldsymbol{a^4=2}$	0	$a^4=2$	$a^8=1$	a^5	a^3	a^2	a^1	a^6	a^7
$\boldsymbol{a^1}$	0	a^1	a^5	a^2	$a^8=1$	a^7	a^6	a^3	$a^4=2$
$\boldsymbol{a^7}$	0	a^7	a^3	$a^8=1$	a^6	a^5	$a^4=2$	a^1	a^2
$\boldsymbol{a^6}$	0	a^6	a^2	a^7	a^5	$a^4=2$	a^3	$a^8=1$	a^1
$\boldsymbol{a^5}$	0	a^5	a^1	a^6	$a^4=2$	a^3	a^2	a^7	$a^8=1$
$\boldsymbol{a^2}$	0	a^2	a^6	a^3	a^1	$a^8=1$	a^7	$a^4=2$	a^5
$\boldsymbol{a^3}$	0	a^3	a^7	$a^4=2$	a^2	a^1	$a^8=1$	a^5	a^6

Пример кодирования над полем Галуа GF (3^2)

Для наглядности кодирования РС кодов (8,4) над полем Галуа GF (3^2) приведем пример. Пусть информационный полином состоит из 4 пары тритов: 22 21 11 01, нужно его закодировать, для этого выполним последовательность операций:

1) Переведем $S(x)$ с троичного вида в степенной вид по таблице 4.5:

$S(x)=\overline{22210111}=\overline{a^3a^2a^8a^7}$.

2) К $S(x)$ припишем $2t=r=4$ нулей:

$T(x)=S(x)x^4=\overline{a^3a^2a^8a^70000}$.

3) С помощью таблицы 4.6, таблицы 4.7 выполним деление $T(x)$ на рассчитанный выше $g(x)$. Найдем остаток $R(x)$ от деления $T(x)$ на $g(x)$:

$$
\begin{array}{l|l}
a^3x^7+a^2x^6+a^8x^5+a^7x^4 & a^8x^4+a^7x^3+a^2x^2+a^4x+a^2 \\
\underline{a^3x^7+a^2x^6+a^5x^5+a^7x^4+a^5x^2} & a^3x^3+a^7x+a^2 \quad - \ Q(x) \\
a^7x^5+a^1x^3 & \\
\underline{a^7x^5+a^6x^4+a^1x^3+a^3x^2+a^1x} & \\
a^2x^4+a^7x^2+a^5x & \\
\underline{a^2x^4+a^1x^3+a^4x^2+a^6x+a^4} & \\
R(x) - \quad a^5x^3+a^6x^2+a^7x+a^8 &
\end{array}
$$

Ответ, $R(x)=\overline{a^5a^6a^7a^8}$.

4) С помощью таблицы 4.6 рассчитаем $C(x)$:

$C(x)=Q(x)g(x)=T(x)-R(x)=\overline{a^3a^2a^8a^70000}-\overline{a^5a^6a^7a^8}=\overline{a^3a^2a^8a^7a^1a^2a^3a^4}$.

По таблице 4.5 переведем полученное значение в троичный вид, который и будет закодированной последовательностью:

$C(x)=\overline{a^3a^2a^8a^7a^1a^2a^3a^4}=\overline{2221011110212202}$.

Пример декодирования над полем Галуа GF (3^2)

Для декодирования РС кодов (8,4) над полем Галуа GF (3^2) приведем пример. Пусть на закодированный полином, полученный в предыдущем примере, $C(x)=\overline{2221011110212202}$ (в степенном виде $C(x)=\overline{a^3a^2a^8a^7a^1a^2a^3a^4}$) воздействовал

шум $e(x)=\overline{0021000000110000}$ (в степенном виде $e(x)=\overline{0a^2000a^700}$), в результате получен многочлен $Y(x)$:

$$Y(x)=C(x)+e(x)=\overline{2221011110212202}+\overline{0021000000110000}=\overline{2212011110022202}.$$

Многочлен в степенном и полиномиальном видах $Y(x)=\overline{a^3a^6a^8a^7a^1a^4a^3a^4}=$ $=a^3x^7+a^6x^6+a^8x^5+a^7x^4+a^1x^3+a^4x^2+a^3x+a^4$, с помощью РС-кодов (8,4) нужно декодировать и исправить $Y(x)$. Для этого выполним последовательность операций:

1) Вычислим компоненты синдрома ошибки $S(x)$, используя соотношение $a^8=1$ и таблицы 4.6, таблицы 4.7:

$$s_1=Y(a^1)=a^{10}+a^{12}+a^{13}+a^{11}+a^4+a^6+a^4+a^4=a^2+a^4+a^5+a^3+a^4+a^6+a^4+a^4=$$

$$=a^5+a^6+a^7+a^8=a^4+a^6=a^7;$$

$$s_2=Y(a^2)=a^{17}+a^{18}+a^{18}+a^{15}+a^7+a^8+a^5+a^4=a^1+a^2+a^2+a^7+a^7+a^8+a^5+a^4=$$

$$=a^8+a^4+a^6+a^3=0+a^8=a^8.$$

Аналогично вычислим другие компоненты синдрома ошибки.

$s_3=Y(a^3)=a^3$; $s_4=Y(a^4)=a^4$.

Итак, синдром ошибки $S(x)=\overline{a^4a^3a^8a^70}=a^4x^4+a^3x^3+a^8x^2+a^7x$.

2) Вычислим локатор ошибки по алгоритму Берлекэмпа-Месси [51, с.64], используя таблицу 4.5, таблицу 4.6, таблицу 4.7.

Для этого, введем некоторые переменные и их начальные значения: $r=0$ - номер итерации, $L=0$, $B(x)=1$ - нормирующая добавка, $L(x)=1$ - начальный локатор ошибки. Во время выполнения каждой из $2t$ итераций, значения будут изменяться пока не получим окончательный вариант локатора ошибки.

Выполнение каждой итерации:

1. Для $r=1$ сначала найдем Δr - ошибку в следующем компоненте синдрома:

$$\Delta r=\sum_{j=0}^{L}L_js_{r-j}=\sum_{j=0}^{0}L_js_{1-j}=L_0s_1=1\cdot a^7=a^7.$$

Поскольку $\Delta r\neq 0$ вычислим новый многочлен связей:

$M(x)=L(x)-\Delta r\cdot x\cdot B(x)=1-a^7\cdot x\cdot 1=a^3x+1$.

Поскольку выполняется неравенство $2L=0\le(r-1)=0$ вычислим новую $B(x)$, $L(x)$ и L: $B(x)=\Delta r^{-1}\cdot L(x)=a^{-7}\cdot 1=a^1$, $L(x)=M(x)=a^3x+1=\overline{a^3a^8}$, $L=r-L=1-0=1$.

Так как $r\neq 2t$, переходим к следующей итерации $r=r+1=2$

2. Для $r=2$ находим Δr:

$$\Delta r=\sum_{j=0}^{L}L_js_{r-j}=\sum_{j=0}^{1}L_js_{2-j}=L_0s_2+L_1s_1=a^8\cdot a^8+a^3\cdot a^7=a^8+a^2=a^3$$

Поскольку $\Delta r\neq 0$, вычислим новый многочлен связей:

$M(x)=L(x)-\Delta r\cdot x\cdot B(x)=a^3x+a^8-a^3\cdot x\cdot a^1=a^3x+a^8-a^4x=a^5x+a^8$

Поскольку неравенство $2L=1\le(r-1)=1$ не выполняется, вычислим новые ошибки $L(x)$ и $B(x)$: $L(x)=M(x)=a^5x+a^8=\overline{a^5a^8}$, $B(x)=x\cdot B(x)=x\cdot a^1=\overline{a^10}$.

Так как $r \neq 2t$ переходим к следующей итерации $r = r + 1 = 2$

3. Для $r = 3$ аналогично находим $B(x)$, $L(x)$ и L:

$B(x) = a^7 x + a^2 = \overline{a^7 a^2}$, $L(x) = a^3 x^2 + a^5 x + a^8 = \overline{a^3 a^5 a^8}$, $L = r - L = 3 - 1 = 2$.

4. Для $r = 4$ аналогично находим $B(x)$, $L(x)$ и L:

$B(x) = a^7 x^2 + a^2 x = \overline{a^7 a^2 0}$, $L(x) = a^8 x^2 + a^8 = \overline{a^8 0 a^8}$, $L = 2$.

Так как $r = 2t = 4$ окончательный локатор ошибки $L(x) = \overline{a^8 0 a^8} = a^8 x^2 + a^8$

3) Находим корни локатора ошибки с помощью алгоритма Чэня [51, с.65, 60, с.102], для этого используя таблицу 4.6, таблицу 4.7 последовательно вычислим $L(a^{-j})$ для каждого $j = 1,...,q-1$. Если $L(a^{-j}) = 0$, то элемент Y_j кодовой комбинации $Y(x)$ содержит ошибку:

$L(a^{-7}) = L(a^1) = a^{10} + a^8 = a^2 + a^8 = a^3 \neq 0$;

$L(a^{-6}) = L(a^2) = a^{12} + a^8 = a^4 + a^8 = 0$ - ошибка в Y_6;

$L(a^{-5}) = L(a^3) = a^{14} + a^8 = a^6 + a^8 = a^1 \neq 0$;

$L(a^{-4}) = L(a^4) = a^{16} + a^8 = a^8 + a^8 = a^4 \neq 0$;

$L(a^{-3}) = L(a^5) = a^{18} + a^8 = a^2 + a^8 = a^3 \neq 0$;

$L(a^{-2}) = L(a^6) = a^{20} + a^8 = a^4 + a^8 = 0$ - ошибка в Y_2;

$L(a^{-1}) = L(a^7) = a^{22} + a^8 = a^6 + a^8 = a^1 \neq 0$;

$L(a^0) = L(a^8) = a^{24} + a^8 = a^8 + a^8 = a^4 \neq 0$.

Итак, нашли, что в Y_6-м и Y_2-м элементе кодовой комбинации ошибки, которые отвечают $e(x)$.

4) Определим характер ошибки с помощью алгоритма Форни [51, с.65], используя таблицу 4.6, таблицу 4.7. Для этого сначала вычислим многочлен значений ошибок $W(x)$:

$$W(x) = s(x) \cdot L(x) \bmod x^{2t} = (a^4 x^3 + a^3 x^2 + a^8 x + a^7) \cdot (a^8 x^2 + a^8) \bmod x^4 =$$

$$= (a^4 x^5 + a^3 x^4 + a^8 x + a^7) \bmod x^4 = a^8 x + a^7 = \overline{00 a^8 a^7}.$$

Находим производную от $L(x)$: $L'(x) = (a^8 x^2 + a^8)' = 2a^8 x = a^4 x$.

Находим корректирующий полином, для этого в формулу $e'_l = -\dfrac{W(X_l^{-1})}{L'(X_l^{-1})}$ вместо X_l^{-1} подставим найденные в 3 пункте степени a, при которых $L(a^{-j}) = 0$:

$$e'_6 = -\frac{W(a^{-6})}{L'(a^{-6})} = \frac{W(a^2)}{L'(a^2)} = \frac{a^{10} + a^7}{a^6} = \frac{a^2 + a^7}{a^6} = \frac{a^4}{a^6} = a^{-2} = a^6;$$

$$e'_2 = -\frac{W(a^{-2})}{L'(a^{-2})} = \frac{W(a^6)}{L'(a^6)} = \frac{a^{14} + a^7}{a^{10}} = \frac{a^6 + a^7}{a^2} = \frac{a^5}{a^2} = a^3.$$

Итак, корректирующий полином $e'(x) = \overline{0a^6 000 a^3 00} = \overline{0012000000220000}$.

5) Исправляем ошибки в $Y(x)$. Для этого корректирующий полином $e'(x)$ складываем с $Y(x)$, используя таблицу 4.6:

$$C'(x) = Y(x) + e'(x) = \overline{a^3 a^6 a^8 a^7 a^1 a^4 a^3 a^4} + \overline{0a^6 000 a^3 00} = \overline{a^3 a^2 a^8 a^7 a^1 a^2 a^3 a^4} = C(x)$$

Итак, $C'(x) = C(x)$, то есть с помощью РС-кодов (8,4) над полем Галуа *GF (3²)* было исправлено 2 ошибочные пары тритов. Теперь для получения начального информационного полинома отбрасываем четыре пары проверочных тритов и

получим $S'(x) = \overline{a^3 a^2 a^8 a^7} = \overline{22210111}$, что и является начальным информационным полиномом.

Экспериментальные результаты

При передаче информации квантовым каналом нужно учитывать особенности квантового шума. Одной из основных моделей квантового шума является модель деполяризующего канала, описанная в [48, с.8]. Согласно этой модели, в квантовом канале при передаче чистое состояние отдельного кубита (кудита) с вероятностью p деполяризуется, то есть его состояние становится полностью смешанным (возникает ошибка), а с вероятностью $(1-p)$ состояние кубита (кудита) остается неизменным. Аналогично, при передаче кутрита, который находится в перепутанном состоянии с другим кутритом, деполяризация в квантовом канале приводит к изменению всего перепутанного состояния [51, с.62]. Поэтому, исследовалась корректирующая способность троичных РС-кодов в зависимости от вероятности деполяризации p. Результаты исследования приведены в таблице 4.8, а также на рисунках 4.10 -4.12.

Таблица 4.8 - Испытания корректирующей способности РС-кодов (8,4) над полем Галуа $GF(3^2)$

P	Количество передаваемых блоков по 8 пар кутритов	Количество переданных пар кутритов		Процент переданных пар кутритов без ошибок	Количество переданных блоков данных по 8 пар кутритов		Процент переданных блоков без ошибок
		без ошибок	с ошибками		без ошибок	с ошибками	
0	1000000	8000000	0	100	1000000	0	100
0,05	1000000	7600105	399895	95,0013	994179	5821	99,4179
0,1	1000000	7198339	801661	89,9792	961506	38494	96,1506
0,15	1000000	6799046	1200954	84,9880	894519	105481	89,4519
0,2	1000000	6400722	1599278	80,0090	797656	202344	79,7656
0,25	1000000	6000164	1999836	75,0020	678759	321241	67,8759
0,3	1000000	5597119	2402881	69,9639	551034	448966	55,1034
0,35	1000000	5196660	2803340	64,9582	426666	573334	42,6666
0,4	1000000	4798706	3201294	59,9838	314579	685421	31,4579
0,45	1000000	4400166	3599834	55,0020	220449	779551	22,0449
0,5	1000000	3998354	4001646	49,9794	144018	855982	14,4018
0,55	1000000	3600062	4399938	45,0007	88577	911423	8,8577
0,6	1000000	3198925	4801075	39,9865	49676	950324	4,9676
0,65	1000000	2800679	5199321	35,0084	24998	975002	2,4998
0,7	1000000	2399026	5600974	29,9878	11279	988721	1,1279
0,75	1000000	1999520	6000480	24,9940	4265	995735	0,4265
0,8	1000000	1599767	6400233	19,9970	1206	998794	0,1206
0,85	1000000	1200305	6799695	15,0038	240	999760	0,024
0,9	1000000	801655	7198345	10,0206	19	999981	0,0019
0,95	1000000	399902	7600098	4,9987	0	1000000	0
1	1000000	0	8000000	0	0	1000000	0

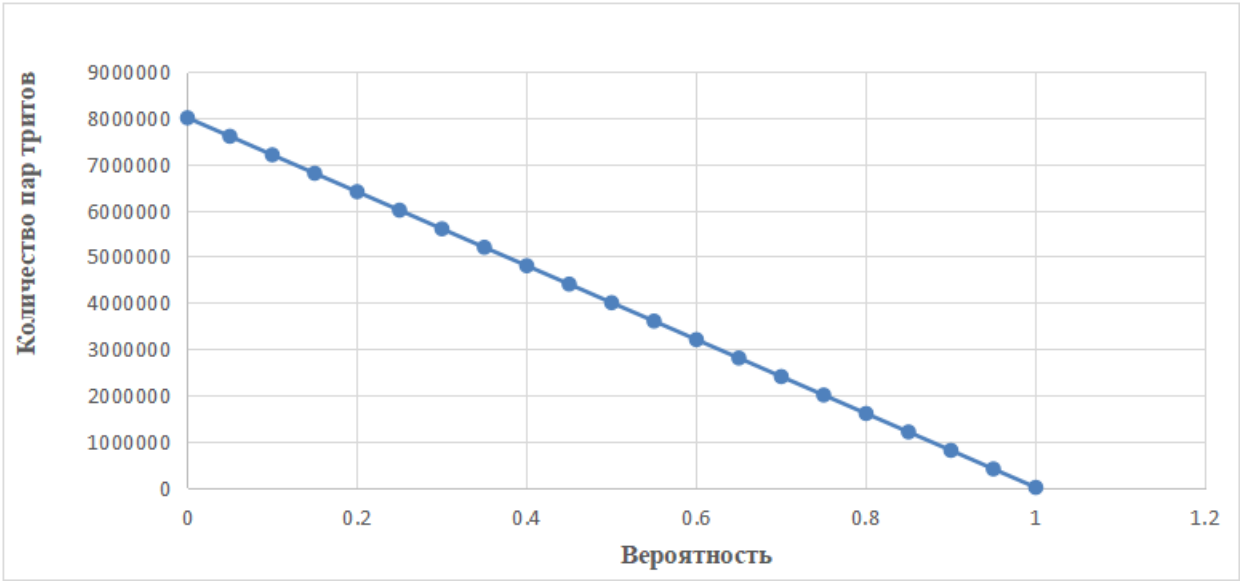


Рисунок 4.10 – Зависимость количества пар, переданных кутритов от вероятности деполяризации

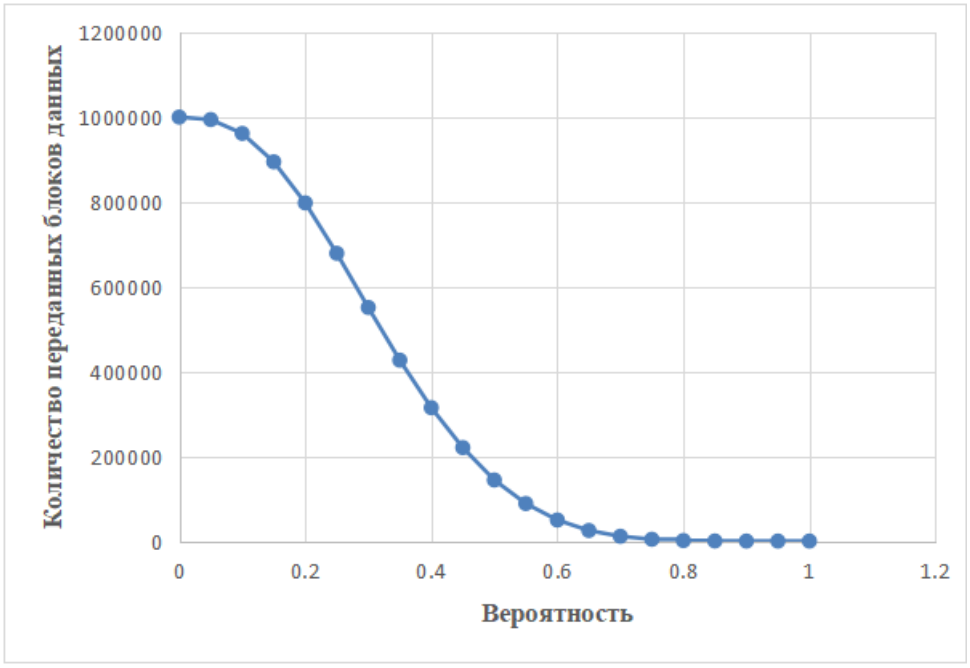


Рисунок 4.11 – Зависимость количества блоков, переданных кутритов от вероятности деполяризации

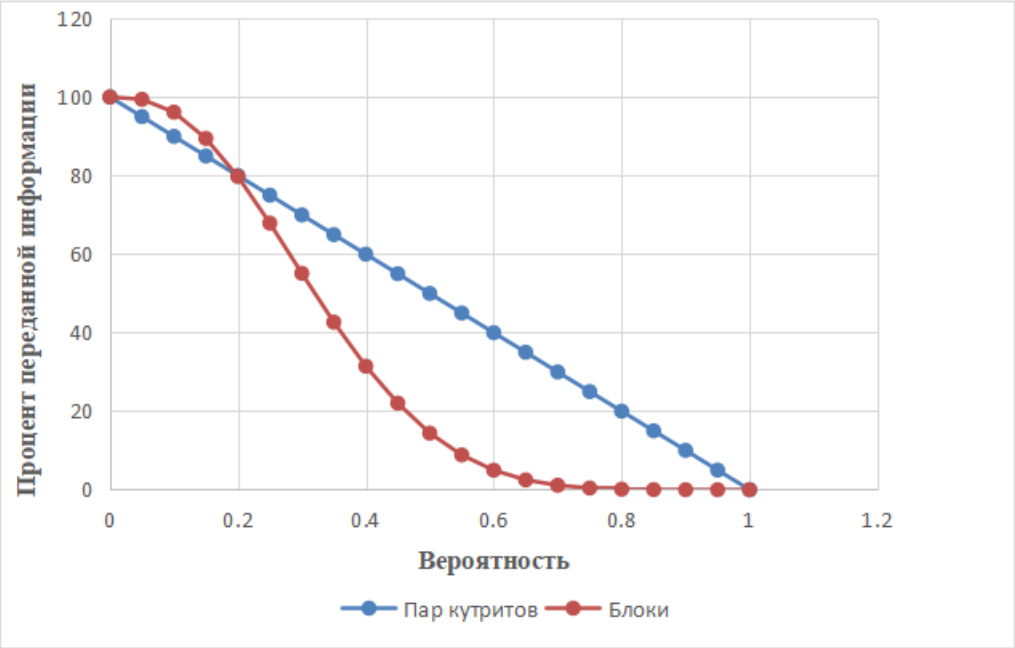


Рисунок 4.12 – Процентное соотношение переданной информации (пар и блоков кутритов) без ошибок в зависимости от вероятности деполяризации

На каждом этапе исследования регистрируем вероятности деполяризации p, далее имитируем процесс передачи квантовым каналом информации, предварительно закодированной троичными РС-кодами, парами перепутанных кутритов. Перебор значений p осуществляем с шагом 0,01. При помощи псевдослучайного тритового генератора, предложенного в [75, с.69], генерируем передаваемую информацию в виде последовательности троичных данных, далее делим на блоки по четыре пары тритов. Затем выполняем их кодирование РС-кодами (8,4) над полем Галуа $GF(3^2)$, в результате каждый блок расширен до восьми пар тритов, которые попарно передаются квантовым каналом. Для каждого p переданы 10^6 таких блоков. С заданной вероятностью p имитируются ошибки при передаче каждой пары тритов, при этом значение пары тритов изменялось случайным образом на один из остальных восьми возможных, что соответствует изменению состояния перепутанных пар кутритов вследствие деполяризации в квантовом канале. После получения блоков выполняется их декодирование РС-кодами. Если при декодировании оказывается, что количество ошибочных пар тритов в каждом блоке не более двух – РС-коды их исправляют, в противном случае декодировать блок невозможно. Данные о количестве полученных и исправленных ошибок, количестве блоков, которые были успешно декодированы и которые невозможно декодировать, собраны в виде статистики (см. таблицу 4.8).

Таким образом, выполненные исследования, которые в совокупности позволяют повысить уровень доступности системы КПБС минимум на 38%. В работе формализована тритовая система помехоустойчивого кодирования, исследована работа системы КПБС на основе разработанного детерминистического протокола с парами полностью перепутанных кутритов в режиме передачи сооб-

щений. На основе данных исследований разработана математическая модель системы КПБС с применением помехоустойчивых РС-кодов над конечным полем Галуа *GF* (3^2) в режиме передачи сообщений [55, с. 150].

Кроме того, разработано программное обеспечение, с помощью которого проведено имитационное моделирование работы данной системы КПБС. В результате моделирования получены статистические данные, подтверждающие пригодность данных кодов для коррекции ошибок (при небольшом уровне природных шумов в квантовом канале) и способность обеспечивать высокую доступность квантового канала при реализации типовых протоколов [55, с.152].

Кроме того, подробно рассмотрено использование троичных РС-кодов и выполнена оценка их корректирующей способности при передаче информации с использованием перепутанных пар кутритов в квантовом канале с шумом.

Полученная, в результате экспериментального исследования, статистическая информация показывает, что предложенные авторами троичные коды хорошо справляются с коррекцией ошибок, если вероятность деполяризации кутрита в квантовом канале не превышает 20-25%.

Поскольку в современных экспериментах уровень ошибок при передаче фотонов квантовым каналом, как правило, не превышает нескольких процентов (в частности 7-10%), то предложенные троичные РС-коды являются пригодными для помехоустойчивого кодирования в детерминистических квантово-криптографических протоколах, которые базируются на использовании кутритов [51, с. 62, 86-88].

4.3 Эксперименты с квантовыми протоколами распределения ключей

Эксперименты проводились в специализированной лаборатории Белорусской государственной академии связи (Минск, Беларусь). Для исследования работы квантовых протоколов BB84 и B92 использовалась экспериментальная установка квантовой системы, структурная схема которой представлена на рисунке 4.13 (реализация детерминистических протоколов не проводилась, поскольку для этого требовались нелинейные кристаллы и квантовая память), используя теоретические наработки [89-103]. Носителями информации в протоколе BB84 являются фотоны, поляризованные под углами 0º, 45º, 90º и 135º.

Для выполнения экспериментов пользователями 1 и 2 произвольно и независимо друг от друга были выбраны углы поляризации и сгенерированы фотоны со случайной поляризацией.

Далее осуществляется регистрация и прием вторым пользователем сигнала. При этом пользователи случайным образом выбирают один из видов угла измерения поляризации: диагональный или перпендикулярный. Диагональный – 45º или 135º. Перпендикулярный – 0º или 90º. При этом фотоны с 0º и 45º -й поляризацией принимают за двоичный «0», а с 90º и 135º -й поляризацией принимают за двоичную «1». Первый пользователь по открытому каналу принимает информацию от второго пользователя о виде выбранного угла, т.е. диагональный или перпендикулярный был выбран угол для регистрации каждого фотона, при этом не разглашает сами результаты измерения. Затем сообщает пользователю по

тому же открытому каналу правильно ли был выбран вид угла измерения для каждого фотона. По результатам измерений далее пользователи 1 и 2 отбрасывают те случаи, когда измерения второго пользователя были неверны. Оставшиеся верные результаты переводят в двоичные значения – «1» или «0», таким образом формируя секретный ключ.

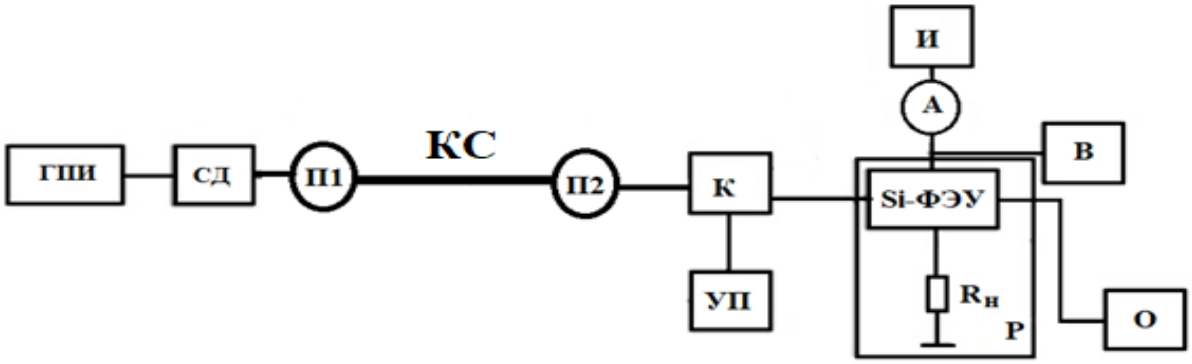


Рисунок 4.13 – Структурная схема установки КРК

На рисунке 4.13 используются следующие обозначения: КС – канал связи, ГПИ – генератор прямоугольных импульсов, СД – светодиод, П1и П2 – поляризаторы, А – амперметр, В- вольтметр, И – источник питания, S_i – ФЭУ- кремниевый фотонный умножитель, Р – регистратор сигналов, УП – блок управления, О- осциллограф, К- коммутатор, $R_н$ – резистор нагрузки [86].

На следующих рисунках (см. рисунки 4.14 – 4.17) представлена экспериментальная установка квантовой системы и ее ключевые компоненты [92].

Рисунок 4.14 – Экспериментальная установка квантовой системы

Рисунок 4.15 – Подключение к квантовой системе ПО цифровой осциллограф

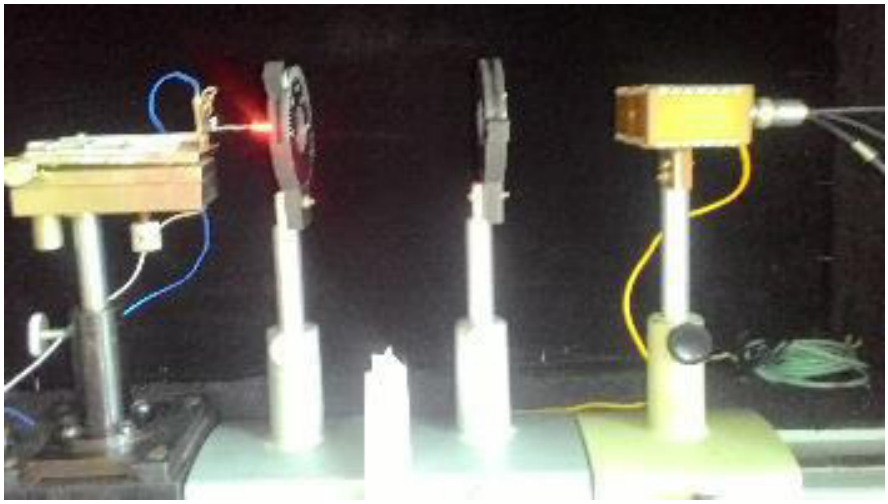


Рисунок 4.16 – Светодиод, поляризаторы и регистратор сигналов

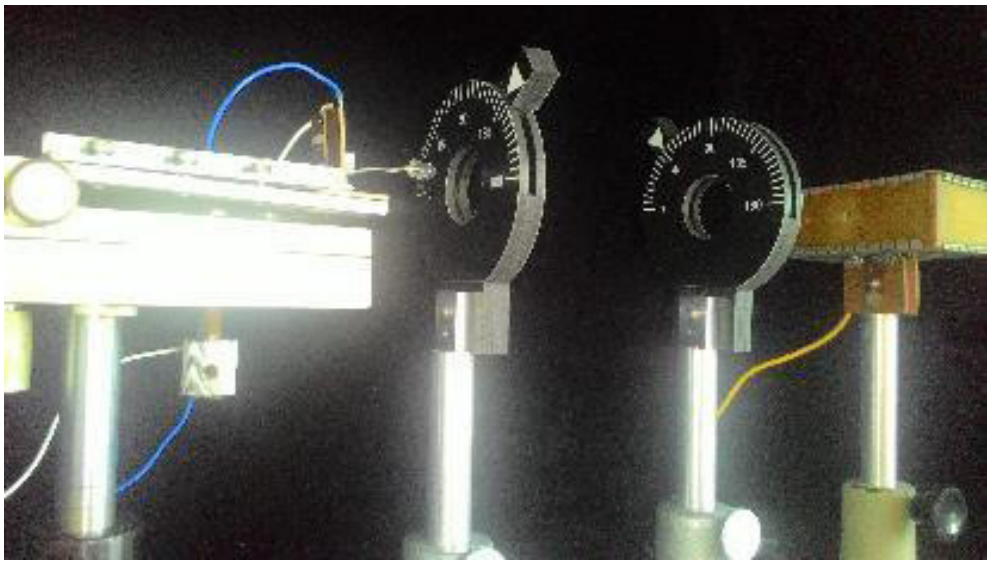


Рисунок 4.17 – Поляризаторы фотонов

Выполняются следующие шаги:

1 шаг. Выбор угла поляризации. Данные эксперимента представлены в виде таблицы 4.9.

Таблица 4.9 – Выбор угла поляризации

Пользователь 1	Углы поляризации, °	Пользователь 2	Углы поляризации, °
1	0	1	45
2	45	2	135
3	135	3	90
4	90	4	0
5	90	5	90
6	90	6	0
7	45	7	45
8	135	8	135
9	0	9	135
10	90	10	90
11	0	11	90
12	45	12	45
13	135	13	0
14	90	14	0
15	0	15	135
16	135	16	45
17	45	17	90
18	0	18	45
19	90	19	45
20	45	20	0

2 шаг. Выполняется регистрация фотонов и обмен информацией о выбранном угле поляризации и фиксирование результата (таблица 4.10.).

Таблица 4.10 – Определение вида поляризации

Пользователь 1	Пользователь2
1	2
В	Д
Д	В
Д	В
В	В
В	В
В	В
Д	Д
Д	Д
В	Д
В	В
В	В
Д	Д
Д	В

Продолжение таблицы 4.10

1	2
В	В
В	Д
Д	Д
Д	В
В	Д
В	Д
Д	В

Отбрасываются неудачные попытки и фиксируются удачные, затем производится их кодирование (таблица 4.11). При совпадении углов поляризации на осциллографе будет сигнал, представленный на рисунке 4.18, в случае если углы поляризации не совпадают, то на осциллограмме будет сигнал, представленный на рисунке 4.19. В том случае, когда фиксируется 50% сигнал, то на осциллограмме будет сигнал, который представлен на рисунке 4.20.

Таблица 4.11 – Принятие решения и получение ключа

Пользователь 1	Пользователь 2	Решение	Прием	Ключ
1	2	3	4	5
В	Д	нет		
Д	В	50%		
Д	В	нет		
В	В	50%		
В	В	нет		
В	В	нет		
Д	Д	100%	v	0
Д	Д	100%	v	1
В	Д	нет		
В	В	100%	v	1
В	В	нет		
Д	Д	100%	v	0
Д	В	нет		
В	В	нет		
В	Д	нет		
Д	Д	нет		
Д	В	нет		
В	Д	нет		
В	Д	нет		
Д	В	50%		

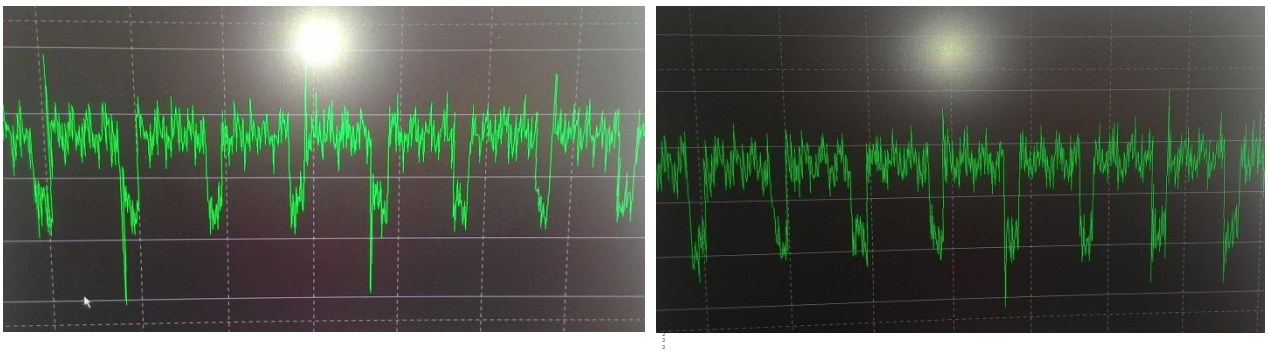


Рисунок 4.18 – Удачная 100% регистрация на осциллографе сигнала

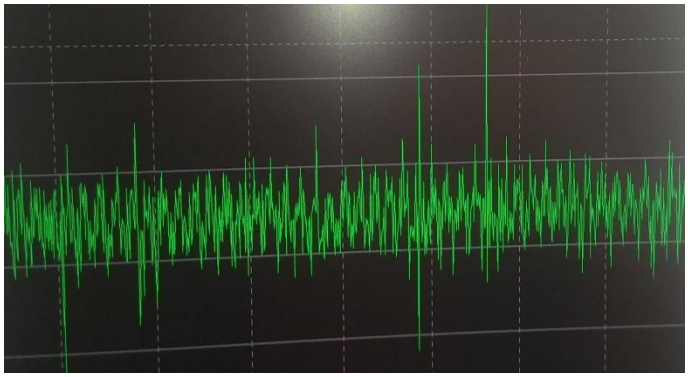


Рисунок 4.19 – Неудачная регистрация на осциллографе сигнала

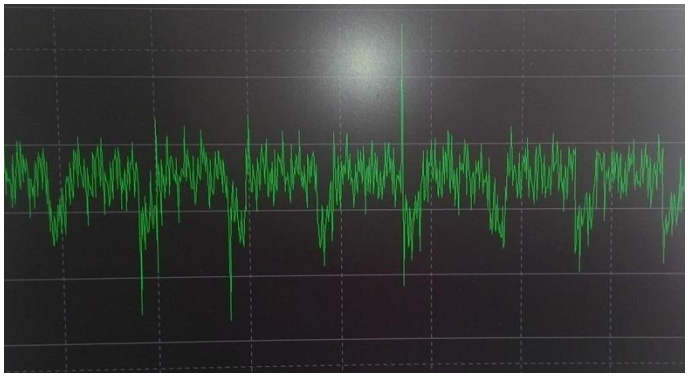


Рисунок 4.20 – 50 % регистрация на осциллографе сигнала

При исследовании протокола B92, так же используются диагональная и перпендикулярная поляризация. Все действия выполняются аналогично. Но в данном протоколе 1 пользователь берет только два угла поляризации: 0º, 45º. А второй пользователь берет углы поляризации 90º и 135º. При этом фотоны, поляризованные под углом 0º используется для передачи двоичного 0, а фотоны, поляризованные под углом 45º - для передачи двоичной 1. Если при выборе перпендикулярного вида угла, т.е. 90º, регистрируется событие, то 2 пользователь знает, что послан фотон с углом поляризации 45º, и записывается в последовательность двоичная 1. Если при выборе диагонального угла поляризации, 135º, регистрируется событие, то 2 пользователь знает, что послан фотон с углом поляризации

0º, и записывается в последовательность двоичный 0. Остальные результаты измерения считаются нерезультативными и отбрасываются. При работе по такому протоколу нет необходимости согласовывать виды углов поляризации, достаточно сообщить по открытому каналу номера результативных измерений, и тем самым будет генерироваться просеянный ключ. При этом нарушитель, даже получив номера результативных измерений, не сможет правильно определить значение переданного бита, так как кодирующие его состояния являются не ортогональными, и, следовательно, неразличимыми [89, с.115].

4.4 Исследование характеристик оптического волокна

Измерение коэффициента затухания оптического излучения в ОВ

Коэффициент затухания оптического излучения в ОВ измеряется специализированным оборудованием:

- оптический тестер ОТ-2-8;
- рефлектометр МТР 600;
- мобильная измерительная платформа МТР 9000А.

Оптический тестер ОТ-2-8. Тестер позволяет измерить оптическую мощность и затухания в волоконно-оптических линиях связи и компонентах волоконно-оптической техники в диапазонах длин волн от 610 до 1650 нм, а также генерировать стабилизированное оптическое излучение.

Общие характеристики:

- хранение результатов измерений в энергонезависимой памяти с привязкой ко времени и дате проведения измерений (256 ячеек памяти);
- возможность управления измерителем мощности с помощью ПК;
- считывание и просмотр результатов измерений на ПК;
- основные длины волны калибровки 650, 850, 1310, 1490, 1550 и 1625 нм;
- возможность изменения значения длины волны измеряемого оптического излучения на ±40 нм с шагом 5 нм около выбранной центральной длины волны диапазона с целью повышения точности измерения;
- режим измерения относительных уровней;
- два режима работы источника оптического излучения:
    - непрерывный;
    - импульсный с частотой модуляции 2 кГц;
- календарь и часы реального времени;
- индикация состояния аккумулятора;
- автоматическое отключение [92, с.2].

Пределы допустимой относительной погрешности измерения мощности оптического излучения на длинах волн калибровки не превышают:

а) ±12% (±0,49 дБ) на длине волны 650 нм;

б) ±4% (±0,17 дБ) на длине волны 850 нм;

в) ±2,5% (±0,11) на длинах волн 1310, 1490,1550 и 1625 нм.

Таблица 4. 12 -Технические характеристики

Длина волны калибровки, нм	Стандартный диапазон измерений мощности	Высокий диапазон измерений мощности	Высокий диапазон показаний мощности
1	2	3	4
650	от - 30 до +3 дБм (от 1 мкВт до 2 мВт)	от - 10 до +3 дБм (от 100 мкВт до 2 мВт)	от - 10 до +23 дБм (от 100 мкВт до 200 мВт)
850	от - 60 до +3 дБм (от 1 нВт до 2 мВт)	от - 40 до +3 дБм (от 100 нВт до 2 мВт)	от - 40 до +23 дБм (от 100 нВт до 200 мВт)
1310,1550,1490,1625	от - 70 до +7 дБм (от 100 пВт до 5 мВт)	от - 50 до +10 дБм (от 10 нВт до 10 мВт)	от - 50 до +27 дБм (от 10 нВт до 50 мВт)

Пределы допустимой относительной погрешности измерения относительных уровней мощности оптического излучения не превышают:

а) ±6% (±0,25 дБ) на длине волны 650 нм;

б) ±8% (±0,33 дБ) на длине волны 850 нм;

в) ±5% (±0,22) на длинах волн 1310, 1490,1550 и 1625 нм.

Рабочие спектральные диапазоны составляют 850±40 нм, 1310±40 нм, 1550±40 нм.

Пределы допустимой относительной погрешности измерения мощности оптического излучения в рабочих спектральных диапазонах составляют:

а) ±12% (±0,5 дБ) в диапазоне 850±40 нм;

б) ±8% (±0,33 дБ) в диапазонах 1310±40 нм и 1550 ±40 нм.

Дискретность отображения мощности оптического излучения в единице дБм-0,01 дБм.

Дискретность отображения значения мощности оптического излучения, выраженной в милливаттах, микроваттах или нано ваттах представлено в таблице 4.13.

Таблица 4.13 - Дискретность отображения мощности оптического излучения

Диапазон мощности оптического излучения	Дискретность
0,001-9,999 нВт	0,001 нВт
10,00-99,99 нВт	0,01 нВт
100,0-999,9 нВт	0,1 нВт
1,000-9,999 мкВт	0,001 мкВт
10,00-99,99 мкВт	0,01 мкВт
100,0-999,9 мкВт	0,1 мкВт
более 1000 мкВт	1 мкВт

Тестер отображает в децибелах изменение мощности оптического излучения относительно опорного значения с дискретностью 0,01 дБ.

Длина волны источника излучения (ИИ), тип ОВ и оптического разъема и излучаемая мощность для ОТ-2-8 указана в таблице 4.14.

Таблица 4.14 - Длина волн источника излучения

Тестер	Длина волны, нм	Тип ОВ	Мощность излучения, дБм, не менее	Тип оптического разъема ИИ
ОТ-2-8	1310±30	ОМ	-4	FC
	1490±10	ОМ	-4	FC
	1550±30	ОМ	-4	FC
	1625±20	ОМ	-4	FC
	850±20	ММ	-4	ST
	1300±30	ММ	-4	ST

Таблица 4.15- Пределы измерений

Длина волны калибровки, нм	Диапазон измерений мощности, дБм	Мощность источника, дБм
1310,1550,1490,1625	+7÷-70	≥-4
850	+3÷− 60	
650	+3÷− 30	

Рисунок 4.21 - Оптический тестер ОТ-2-8

Источником излучения служит лазерный диод (ЛД), мощность которого стабилизирована с помощью фотодиода обратной связи. Режим работы источника излучения – непрерывный и с модуляцией мощности оптического излучения с частотой 2 кГц.

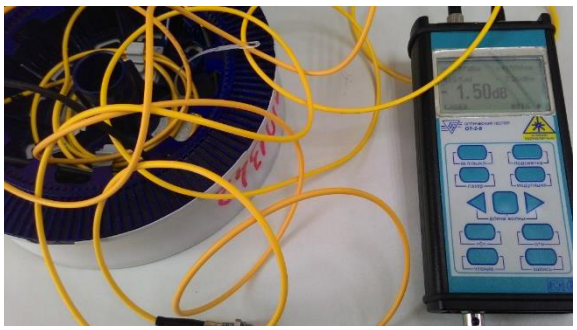


Рисунок 4.22 - Измерения с тестером ОТ-2-8

Для установленной длины волны 1550 nm, принимаемого излучения, мощность составляет - 419,5 μW; мощность в дБ - 1,50, опорное значение 2,26 dDm [92, с.3].

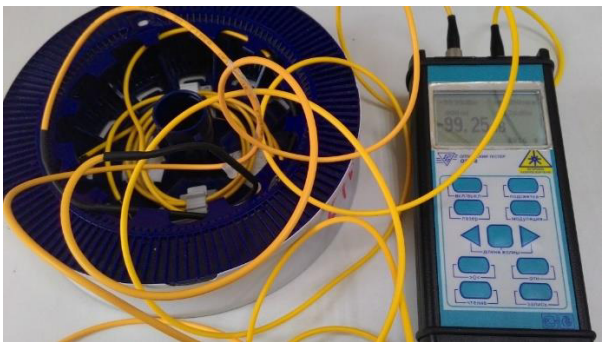


Рисунок 4.23 - Измерения с тестером ОТ-2-8

Опытные измерения показали что для длины волны $\lambda = 1310$ коэффициент затухания составляет *а=0,35* дБ/км. Для длины волны $\lambda = 1310$ коэффициент затухания составляет *а=0,22* дБ/км.

При измерении катушки ОВ длиной 3 км, при использовании оптического разъема с коэффициентом затухания *а ≤0,5* дБ/км, затухание катушки составит $0{,}22 \times 3 = 0{,}66 + 0{,}5 = 1{,}16 дБ$.

Затухание на аттенюаторе *max=26,59дБ; мин=1,10 дБ.*

Затухание на аттенюаторе *max=26,59дБ; min=1,10 дБ.*

При длине длины волны $\lambda = 1310$, с ОВ длиной 1 км, затухание на аттенюаторе *max=27,65дБ; min=1,63* дБ.

При длине длины волны $\lambda = 1310$, с ОВ длиной 4 км, затухание на аттенюаторе *max=29,20 дБ; min=2,21 дБ.*

При длине длины волны $\lambda = 1310$, с ОВ длиной 3 км, затухание на аттенюаторе *max=29,96дБ; min=1,47 дБ.*

Рефлектометр МТР 600. Многофункциональный рефлектометр содержит: оптический рефлектометр; источник оптического излучения; измеритель оптической мощности; источник видимого излучения.

МТР 6000 позволяет производить измерения на одной из трёх длин(ах) волн(ы).

Программное обеспечение прибора позволяет осуществлять анализ проведенного измерения в двух режимах:

- в автоматическом режиме. В этом режиме устанавливаются наиболее подходящие для измеряемой линии параметры измерения, производятся последовательное измерение на активных, для данного прибора, длинах волн и автоматический анализ полученных результатов (поиск неоднородностей и составление таблицы отметок).

- в ручном режиме. Измерение производится после выставления соответствующих измеряемой линии параметров измерения в соответствующем диалоге.

Основные режимы работы с результатами измерений:

- режим измерения затухания/отражения с использованием маркеров;
- режим изменения масштаба с использованием специальной «лупы»;
- режим для сравнения/наложения измеренных рефлектограмм;
- режим просмотра событий (неоднородностей) на рефлектограмме с использованием таблицы отметок.

Полученные результаты можно быстро сохранить на флэш-память прибора, с последующим использованием для работы и анализа [92, с.5].

Таблица 4.16 - Технические характеристики

Характеристики	Значение
1	2
Память	Встроенная (не менее 500 рефлектограмм) / съемный диск USB
Связь с компьютером	USB
Экран	4 , 3 " TFT , 65536 цветов
Питание	аккумуляторная батарея (7 часов) / сетевой блок питания
Габариты, см	20 × 15 × 3
Масса, кг	1 , 5
Длина волны, нм	одномодовое 1310 ± 20 ;1550 ± 20 1625 ± 20 многомодовое 850 ± 20 1300 ± 20
Динамический диапазон (ОСШ = 1), дБ	одномодовое 42 ;43 ;41 многомодовое 23 ;23
Мертвая зона по затуханию 1 , м	7… 12
Мертвая зона по отражению, м	2 … 3 , 5
Длительность импульсов, нс Диапазоны расстояний, км Интервал дискретизации, м	одномодовое 8, 25, 100, 300, 1000, 3000, 10000, 20000 многомодовое 8, 25, 100, 300, 1000 одномодовое 5, 10, 20, 40, 80, 120, 160, 240 многомодовое 5, 10, 20, 40, 80 0 , 16 … 7 ,8
Число отсчетов	до 64 000
Погрешность измерения расстояния, м	± (0,5 + интервал дискретизации + 3/ 10 -5/ L)
Погрешность измерения затухания, дБ/дБ	± 0,05
Тип оптического разъема	FC, SC, ST

Таблица 4.17 - Технические характеристики

Измеритель оптической мощности						
Длины волн калибровки, нм	850			1310, 1550		
Диапазон измерения оптической мощности, дБм	+3 … – 60			+3 … – 65		
Погрешность измерения мощности, дБ	0.33			0.22		
Погрешность измерения относительных уровней мощности, дБ	0.17			0.11		
Встроенный источник видимого излучения						
Выходная мощность, мкВт	›500					
Сменный модуль оптического рефлектометра						
Длина волны, нм	850±20	1300±20	850±20/1300±20	1310±20	1550±20	1310±20/1550±20
Динамический диапазон (ОСШ=1):						
стандартный, дБ	30	29	28.3	36.5	35	36/34.5
высокий, дБ	-	-	-	41.5	39.5	41/39
Мертвая зона при измерении затухании /обнаружении неоднородностей	14.5 /3.5					
Общие параметры платформы						
Питание	аккумуляторная батарея (не менее 6 часов) / 12 / ~220В					
Габариты, мм	243 x 195 x 56					
Масса с аккумуляторной батареей, кг	2.5					

Рисунок 4.24 - Измерение двух соединенных катушек с помощью розетки

С помощью прибора можно выявить «мертвую зону», так для оптического кабеля длиной 1,547 км составляет 0,00626 (626 м).

Рисунок 4.25 - ОВ длиной 3,182 км, мертвая зона составляет - 0,00802, затухание на км – 0,343 дБ/км

Рисунок 4.26 - ОВ длиной 3,134 км, мертвая зона составляет - 0,00797, затухание на км – 0,308

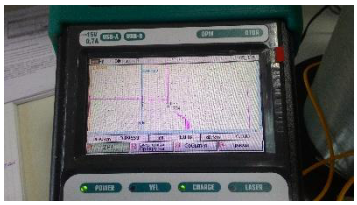


Рисунок 4.27 - ОВ длиной 4,735 км, мертвая зона составляет - 0,0856, затухание на км – 0,338 дБ/км.

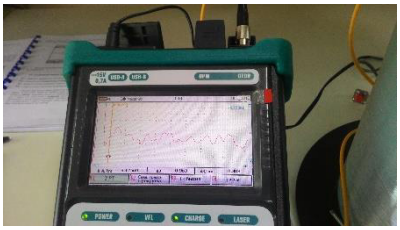


Рисунок 4.28 - ОВ длиной 3,134 км, мертвая зона составляет 0,00797

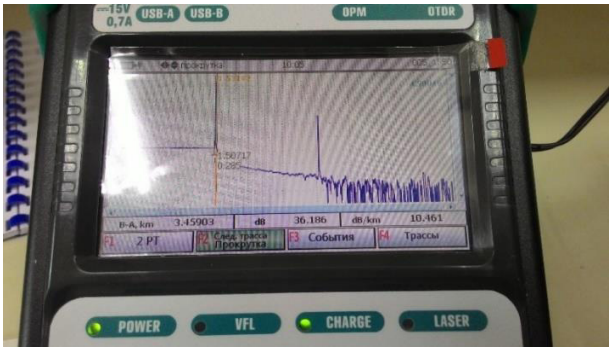


Рисунок 4. 29 - Показания при измерении

Мобильная измерительная платформа MTP 9000A. Многофункциональный оптический прибор - универсальный измерительный прибор, содержит базовый управляющий модуль со встроенным цветным дисплеем и широким набором сменных измерительных модулей, цветной экран с функцией TouchScreen; источник видимого излучения для обнаружения повреждений оптического волокна (VFL).

Рисунок 4.30 - Многофункциональный оптический измерительный прибор MTP 9000A

Сменные модули прибора MTP 9000A:
- оптический рефлектометр:
- модули со стандартным и высоким динамическим диапазоном;
- автоматизация процесса измерения;
- мертвая зона при обнаружении неоднородностей менее 3,5 метра;
- возможность запуска измерений нажатием одной кнопки.

Разработаны модули:
- оптический тестер оптический анализатор спектра;
- анализатор хроматической дисперсии.

Таблица 4.18 - Технические характеристики

Встроенный источник видимого излучения						
Длина волны, нм	650					
Выходная мощность, мкВт	›500					
Сменный модуль оптического рефлектометра						
Длина волны, нм	850±20	1300 ±20	850±20/1300±20	1310±20	1550±20	1310±20/1550±20
Динамический диапазон (ОСШ=1):						
стандартный, дБ	30	29	28/27	36.5	35	36/34.5
высокий, дБ	-	-	-	41.5	39.5	41/39
Мертвая зона при измерении затухании/обнаружении неоднородностей				14.5/3.5		

Продолжение таблицы 4.18

	Общие параметры платформы
Питание	аккумуляторная батарея (не менее 5 часов) / 12 / ~220В
Габариты, мм	243 x 195 x 56
Масса с аккумуляторной батареей, кг	2.5

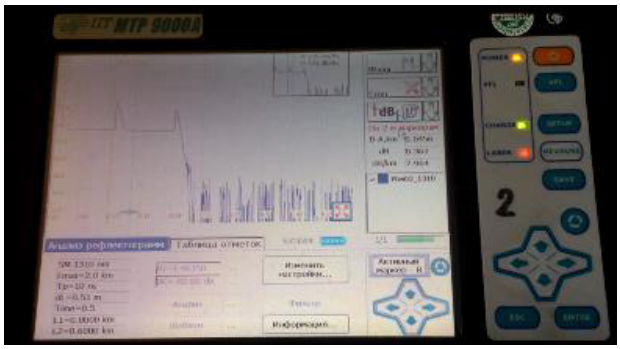


Рисунок 4.31 - Использование устройства MTP 9000A

В качестве эксперимента устройство применялось для выявления утечки в ОВ под влиянием звуковых колебаний. В этих целях использовались: ОВ различных длин; соединители – розетки; колонки усиления звука; генераторы низких и высоких частот; кабели с механическим соединением и т.д. По результату эксперимента можно сделать вывод: для выявления утечки информации из ОВ кабеля под влиянием звукового давления (шумов) необходимо применение высокоточного оборудования. Кроме того, для чистоты проведения эксперимента необходима вакуумная среда, т.е. камера, а также специализированное высокоточное оборудование технических разведок. Только при таких условиях, может быть выявлен факт утечки информации.

Измерение хроматической дисперсии оптического волокна

Хроматическая дисперсия оптических волокон – это зависимость времени распространения оптического излучения в ОВ от длины волны.

Хроматическую дисперсию одномодового ОВ можно измерить прибором Д-2-2/12 (см. рисунок 4.32). В приборе используются 12 измерительных лазерных диодов и номинальные значения длин волн: 1270, 1310, 1330, 1350, 1470, 1490, 1510, 1530, 1550, 1570, 1590, 1610 нм.

Длина измеряемых ОВ составляет от 1 до 150 км. Пределы допустимой абсолютной погрешности измерения коэффициента хроматической дисперсии составляют ± 0,1 пс/(нм·км) при длине ОВ от 1 до 20 км; ± 0,02 пс/(нм·км) при длине ОВ от 20 до 100 км; пределы допустимой абсолютной погрешности измерения длины волны нулевой дисперсии составляют ± 0,5 нм, пределы допустимой абсолютной погрешности измерения наклона кривой коэффициента хроматической дисперсии составляют ± 0,5 %.

В состав комплекта прибора входят:

- измеритель хроматической дисперсии ИД-2-2/Х: оптический передатчик оптический приемник;

- блок питания сетевой;
- 2 аттенюатора оптических волоконных. Затухание составляет от 15 до 25 дБ, разъемы FC/APC;
- 2 кабеля оптических соединительных, длиной по 3 м, разъемы FC/APC;
- 2 розетки FC;
- кабель интерфейсный USB-A – USB-B;
- компакт-диск или USB флэш-память с программным обеспечением;
- руководство по эксплуатации;
- упаковочная сумка.

Измерения хроматической дисперсии оптического волокна выполняются с помощью метода фазового сдвига. Принцип работы прибора основан на измерении фазы синусоидальных оптических сигналов с различными длинами волн, которые проходят через измеряемое ОВ. Далее по полученным значениям фаз рассчитываются задержки во всем диапазоне длин волн и параметры, которые характеризуют хроматическую дисперсию ОВ. Прибор содержит два оптических канала – измерительный и опорный. В измерительный канал включается измеряемое ОВ, в опорный канал – любое другое ОВ из измеряемого оптического кабеля или короткий оптический соединительный кабель. Фазы сигналов разных длин волн в измерительном ОВ сравниваются с фазой опорного сигнала.

Рисунок 4.32 - Прибор ИД-2-2/12

Оптический передатчик прибора ИД-2-2 генерирует синусоидальные оптические сигналы на фиксированных длинах волн. В качестве источников излучения используются лазерные диоды с распределенной обратной связью (РОС ЛД). Структурная схема блока показана на рисунке 4.33.

Мощность излучения лазерных диодов (ЛД) модулируется синусоидальным сигналом генератора с частотой f1. Длина волны и мощность излучения ЛД стабилизируются с помощью термоэлектрических охладителей (ТЭО) и фотодиодов обратной связи. Сигналы ЛД по очереди с помощью оптического переключателя подаются на выход измерительного канала. Часть мощности ЛД с длиной волны 1550 нм постоянно подается на выход опорного канала. Управление оптическим переключателем осуществляется сигналом синхронизации, приходящим по опорному ОВ от оптического приемника прибора ИД-2-2.

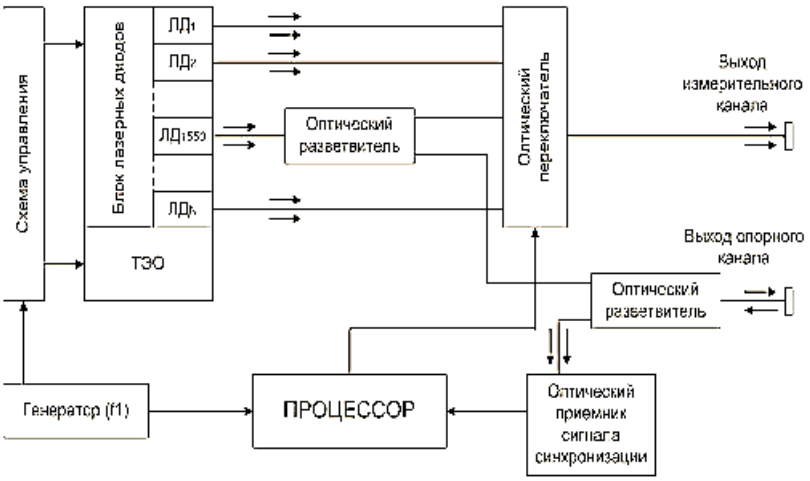


Рисунок 4.33 - Структурная схема блока передатчика

Оптический приемник прибора ИД-2-2 замеряет время распространения сигналов, прошедших через измерительное ОВ. Структурная схема оптического приемника прибора ИД-2-2 показана на рисунке 4.33. Измерительный и опорный сигналы поступают на лавинные фотодиоды (ЛФД) соответствующих оптических приемников, где смешиваются с сигналом генератора с частотой f_2. На выход этих приемников поступает низкочастотный сигнал с разностной частотой: $\Delta f = f_2 - f_1$, $\Delta f << f_1$.

Для согласования амплитуд принимаемых оптических сигналов с диапазоном АЦП в оптический приемник прибора ИД-2-2 встроены переменные электронно-управляемые оптические аттенюаторы (ОА). Процессор также управляет оптическим сигналом синхронизации, который передается в оптический передатчик прибора ИД-2-2 для поочередного включения лазерных диодов и управления оптическим переключателем. Управляющая программа прибора ИД-2-2 осуществляет расчет разности фаз $\Delta\varphi$ принятых сигналов и задержки сигнала данного ЛД (т.е. с данной длиной волны) в измеряемом ОВ: $\tau = -\Delta\varphi/(2\cdot\pi\cdot f_1)$.

По полученным значениям задержек управляющая программа ПК производит расчет параметров хроматической дисперсии ОВ во всем спектральном диапазоне путем аппроксимации результатов измерения методом наименьших квадратов.

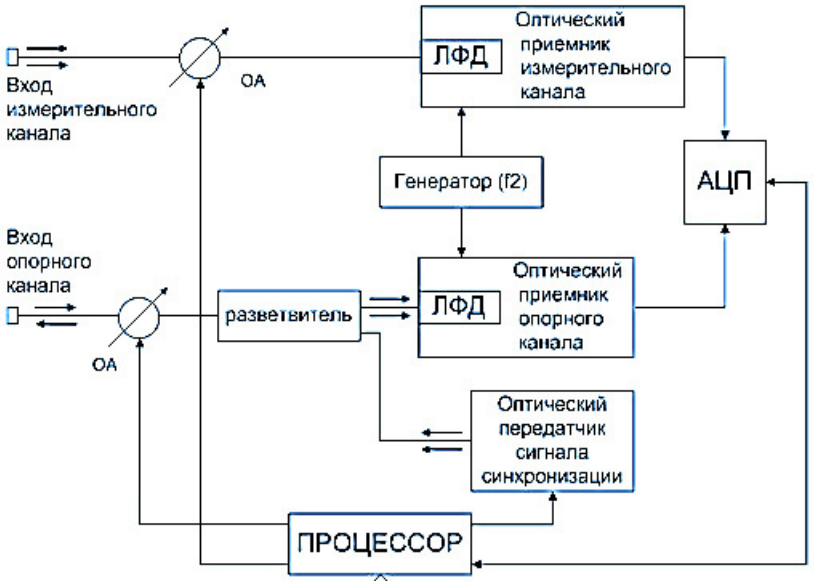


Рисунок 4.34 - Структурная схема оптического приемника прибора ИД-2-2

Этот сигнал преобразуется в цифровую форму с помощью АЦП. Процессор рассчитывает разность фаз этих сигналов и передает в ПК для дальнейшей обработки.

Параметры хроматической дисперсии ОВ указаны на рисунке 4.35 [92, с.8, 96-100].

Параметр	Обозначение/ выражение	Размерность	Примечание
Время распространения сигнала	$\tau(\lambda)$ $\tau(\lambda)/L$	нс нс/км	
Коэффициент хроматической дисперсии	$D(\lambda) = d\tau(\lambda)/d\lambda$ $D(\lambda) = (1/L) \cdot d\tau(\lambda)/d\lambda$	пс/нм пс/(км · нм)	
Длина волны нулевой дисперсии	λ_0	нм	$D(\lambda_0) = 0$
Наклон кривой коэффициента хроматической дисперсии	$S(\lambda) = (1/L) \cdot d\tau^2(\lambda)/d\lambda^2 = (1/L) \cdot D(\lambda)/d\lambda$	пс/(км · нм^2)	

Рисунок 4.35 - Значения параметров хроматической дисперсии ОВ

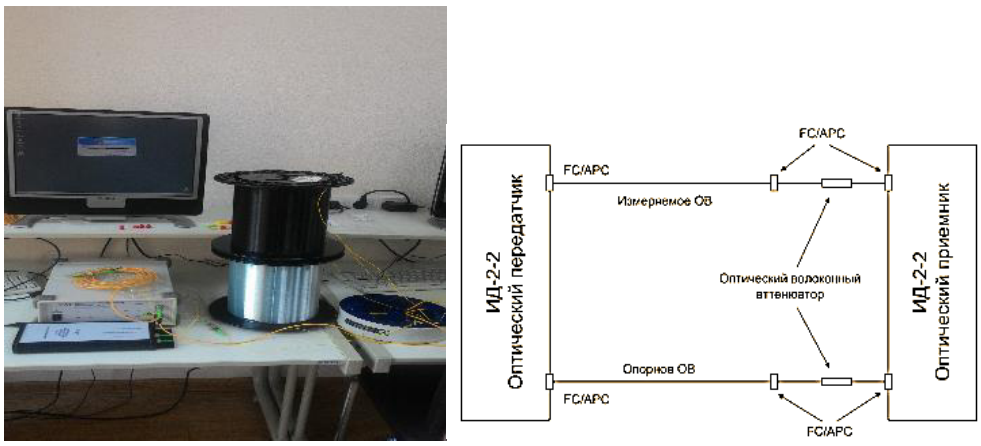


Рисунок 4.36 - Схема подключения ОВ для измерений

Рисунок 4.37 - Прибор ИД-2-2/12 в режиме измерений

При проведении измерений хроматической дисперсии в ОВ, использованы экспериментальная катушка и катушки G652, G657, общая длина составила 7 км 735 м.

Перед проведением измерений проведен контроль соединения волокон.

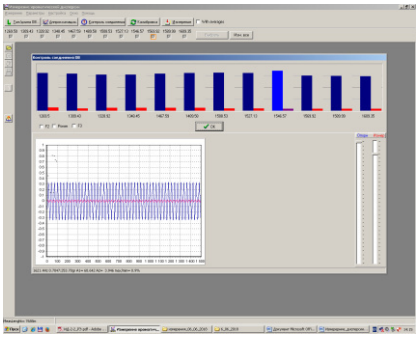


Рисунок 4.38 - Контроль соединения

Затем калибровка и само измерение.

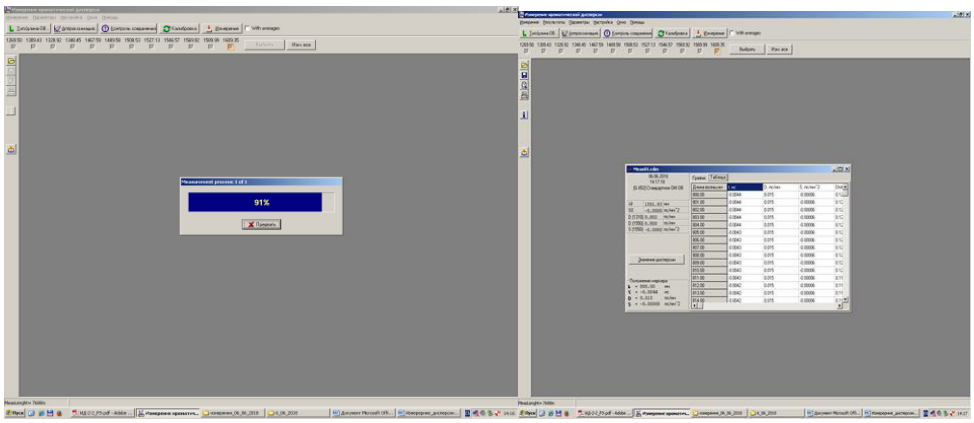


Рисунок 4.39 - Процесс калибровки и измерение дисперсии

В результате получены значения.

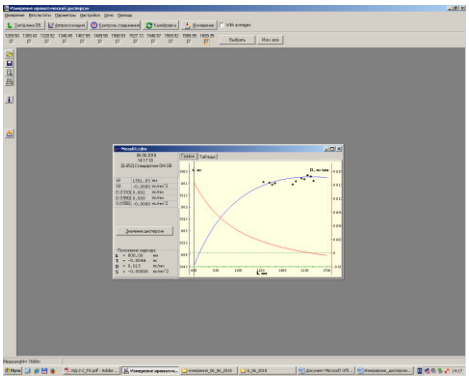


Рисунок 4.40 - Результаты измерений

В результате экспериментальных измерений были получены значения: L, км – длина ОВ; λ_0, нм – длина волны нулевой дисперсии ОВ; *D(λ),* пс/(км*нм) – значение коэффициента хроматической дисперсии на длине волны, указанной в скобках *S_0* или *S(λ),* пс/(км*нм^2) – значение наклона коэффициента хроматической дисперсии на длине волны нулевой дисперсии или на длине волны, указанной в скобках. Dtotal, пс/нм – полное значение коэффициента хроматической дисперсии всего ОВ на длине волны 1310,1550 и 1625 нм (рисунки 4.41 - 4.45).

Для $\lambda = 1310$*: τ(1310) = -0,0010* нс/км; *D(1310)=0,002* пс/нмкм; *S(1310)=-0,00001* пс/(нм^{2}км; *Dtotal(1310)= 0,02* пс/нм;

Для λ = 1550: τ(1550)= -0,0007 нс/км; D(1550) = 0,000 пс/нм*км;

S(15510)=-0,00001 пс/(нм^2*км; *Dtotal(1550)*= 0,00 пс/нм;

Для λ = 1610: τ(1610)= -0,0007 нс/км; D(1610) = 0,000 пс/нм*км;

S(16110)=-0,00001 пс/(нм^2*км; *Dtotal(1610)*= 0,00 пс/нм;

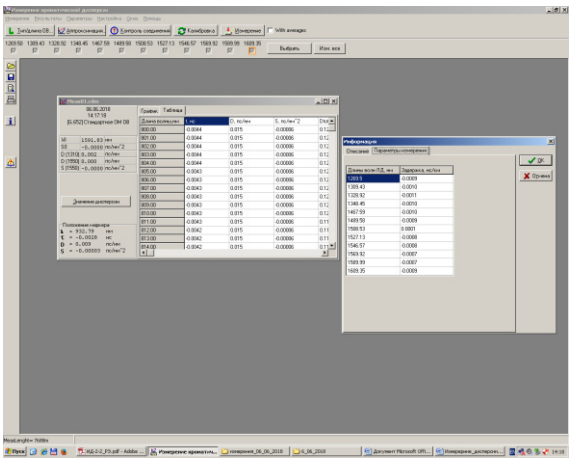


Рисунок 4.41 - Результаты задержек для длин волн от 1269,5 до 1609,35

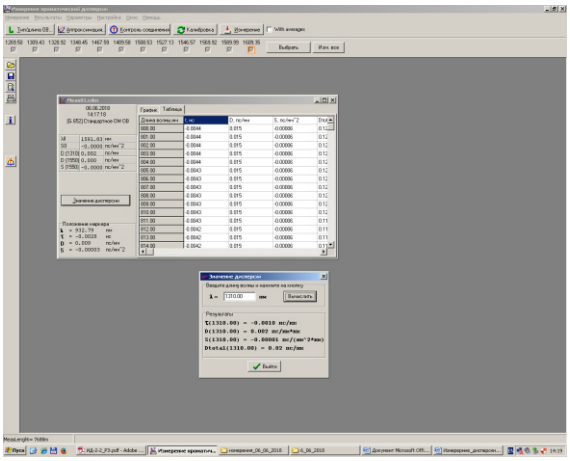


Рисунок 4.42 - Результат хроматической дисперсии для длины волны 1310

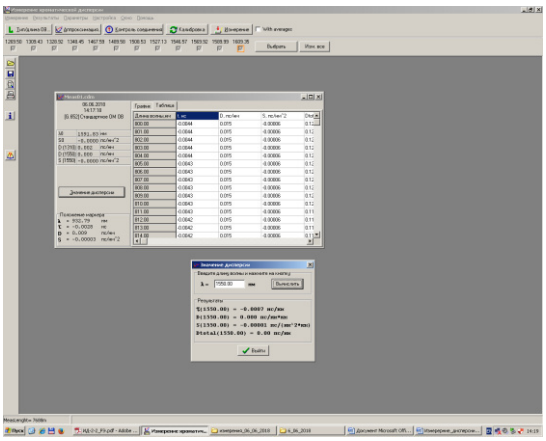


Рисунок 4.43 - Результат хроматической дисперсии для длины волны 1550

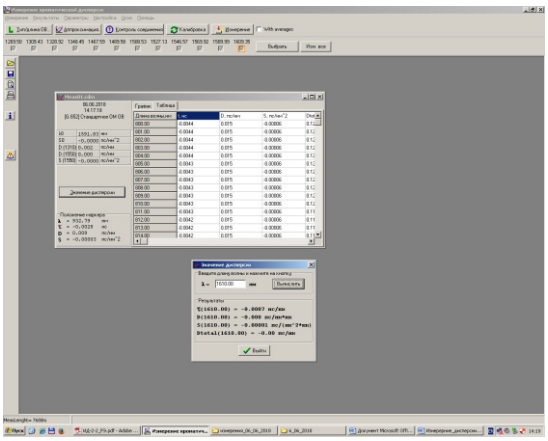


Рисунок 4.44 - Результат хроматической дисперсии для длины волны 1610

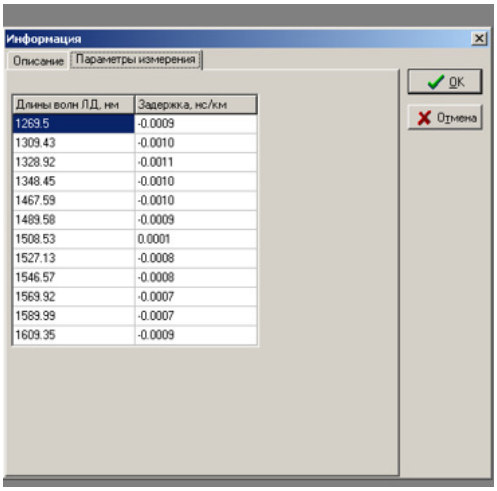


Рисунок 4.45 - Задержка для длин волн

Измерение хроматической дисперсии выявило ее влияние на производительность системы, это явление возникает в связи с различной скоростью распространения длин волн в оптическом волокне. В результате возникает затянутый, неэффективный импульс. При слишком большом значении такой дисперсии происходит перекрестная модуляция и потеря сигнала. Хроматическая дисперсия чувствительна к увеличению длины и числа участков линии связи, а также к увеличению скорости передачи, но на нее не влияют уменьшение частотного интервала между каналами и увеличение числа каналов.

Хроматическую дисперсию можно уменьшить за счет уменьшения абсолютного значения хроматической дисперсии волокна и путем ее компенсации [92, с.12].

Таким образом, в заключительном разделе диссертации были получены следующие результаты:

1) На базе модели квантового детерминистического протокола в режиме контроля подслушивания в среде MATLAB было проведено имитационное моделирование квантового детерминистического протокола в режиме контроля подслушивания и, как результат, удалось повысить скорость распределения ключей

шифрования минимум в 1,52 раза при обеспечении защищенности от некогерентной атаки;

2) На базе квантового детерминистического протокола в режиме передачи сообщений в среде MATLAB было проведено имитационное моделирование квантового детерминистического протокола в режиме передачи сообщений, в результате чего получено подтверждение возможности применения предложенной системы помехоустойчивого кодирования над полем Галуа GF (3^2) при уровне природных шумов до 10%. Также, это позволит повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом минимум на 3,8%.

3) На базе разработанной комбинированной модели режимов контроля подслушивания и передачи сообщений квантового детерминистического протокола был усовершенствован метод безопасного распределения ключей [51, с.66], который является более быстрым, помехоустойчивым и защищенным от некогерентных атак.

4) Также, были сформулированы практические рекомендации по использованию квантовых детерминистических протоколов в квантово-криптографических системах в условиях использования деполяризационного квантового канала и присутствия нарушителя.

5) В результате моделирования получены статистические данные, подтверждающие пригодность кодов Рида-Соломона для коррекции ошибок (при небольшом уровне природных шумов в квантовом канале) и способность обеспечивать высокую доступность квантового канала при реализации типовых протоколов.

6) Кроме этого, были проведены эксперименты с использованием лабораторного оборудования УО «Белорусская государственная академия связи» (Минск, Беларусь), которые заключались в исследовании эффективности протоколов квантового распределения ключей, а также исследовании характеристик одно квантовых фотоприемников, измерении коэффициента затухания оптического излучения и хроматической дисперсии оптического волокна.

ЗАКЛЮЧЕНИЕ

Краткие выводы по результатам диссертационных исследований

В диссертационной работе решена актуальная научно-техническая задача разработки современных методов повышения эффективности распределения ключей шифрования на базе протоколов квантовой криптографии.

Проведенные исследования позволяют сформулировать выводы:

1. В результате анализа современных методов, моделей и коммерческих систем распределения ключей шифрования по критериям безопасности (защищенности) и скорости получена классификация квантово-криптографических методов. Данная классификация за счет расширения множества известных базовых признаков, частичных обобщений теоретических положений и практических достижений в области квантовой криптографии, позволяет расширить возможности по выбору необходимых квантово-криптографических методов для построения безопасных систем распределения ключей шифрования.

2. Разработаны модели угроз и нарушителя в квантово-криптографических системах, которые учитывают специфику и уязвимости систем КК, а также возможности нарушителей в соответствии с текущим и перспективным уровнем вычислительных технологий, позволяющие определить и выбрать наиболее защищенные методы распределения криптографических ключей. В частности, модель угроз позволяет сформировать концептуальные аспекты предупреждения атак и формализовать возможности превентивных систем в процессе их разработки или усовершенствования. Абстрактная модель нарушителя в системах КК позволяет определить совокупность мероприятий различного характера, которые необходимо дополнительно внедрить для обеспечения надежной защиты применяя специфические квантовые системы.

3. Разработана модель квантового детерминистического протокола в режиме контроля подслушивания, которая учитывает особенности квантового канала и вероятности возникновения в нем ошибки в x- и z- базисах измерения, энтропию фон Неймана, а также использует новую процедуру усиления секретности, позволяющую обеспечить безопасное и быстрое распределение ключей (в контексте реализации некогерентной атаки), а также сформулировать практические рекомендации по разработке квантово-криптографических систем в условиях использования деполяризационного квантового канала и присутствия нарушителя. На базе этой модели в среде MATLAB было проведено имитационное моделирование квантового детерминистического протокола в режиме контроля подслушивания и, как результат, удалось повысить скорость распределения ключей шифрования минимум в 1,52 раза при обеспечении защищенности от некогерентной атаки;

4. Разработана модель квантового детерминистического протокола в режиме передачи сообщений, которая за счет формализации системы помехоустойчивого кодирования над полем Галуа $GF(3^2)$ для кутритов, повышения асимптотической стойкости оригинального детерминистического протокола, а также использования алгоритма генерирования троичных псевдослучайных последовательностей, позво-

ляющего повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом и небольшом уровне природных шумов. На базе этой модели в среде MATLAB было проведено имитационное моделирование квантового детерминистического протокола в режиме передачи сообщений, в результате чего получено подтверждение возможности применения предложенной системы помехоустойчивого кодирования над полем Галуа $GF(3^2)$ при уровне природных шумов до 10%. Также, это позволит повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом минимум на 3,8%.

5. Предложен метод усиления секретности с использованием квантовых перепутанных состояний и сгенерированных троичных псевдослучайных последовательностей. В данном методе усиления секретности классическая информация перед ее передачей обрабатывается с помощью квантовых перепутанных состояний, используются сгенерированные троичные псевдослучайные последовательности вместо ресурсоемкого генерирования обратимых матриц над полем Галуа $GF(3^2)$, это позволяет повысить скорость в 22,1 – 36,2 раза (для симметрических криптографических систем с длинной (ключа 128-256 бит) без потери стойкости детерминистических протоколов квантовой криптографии с использованием пар кутритов к некогерентной атаке. Это в свою очередь позволяет повысить скорость передачи без потери стойкости детерминистических протоколов квантовой криптографии с использованием пар кутритов к некогерентной атаке;

6. Реализована комбинированная модель на основе разработанных моделей режима контроля подслушивания и режима передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов с использованием метода усиления секретности, что позволило улучшить метод безопасного распределения ключей, повысить скорость и обеспечить помехоустойчивость деполяризационного квантового канала. В частности усовершенствованный метод усиления секретности, который за счет обработки классической информации перед ее передачей с помощью квантовых перепутанных состояний и использования сгенерированных троичных псевдослучайных последовательностей вместо ресурсоемкого генерирования обратимых матриц над полем Галуа $GF(3^2)$, позволяет повысить скорость в 22,1 – 36,2 раза (для симметрических криптографических систем с длинной (ключа 128-256 бит) без потерь стойкости детерминистических протоколов квантовой криптографии с использованием пар кутритов устойчивых к некогерентной атаке.

7. Кроме этого, были проведены эксперименты с использованием лабораторного оборудования УО «Белорусская государственная академия связи» (Минск, Беларусь), которые заключались в исследовании эффективности протоколов квантового распределения ключей, а также исследовании характеристик одно квантовых фотоприемников, измерении коэффициента затухания оптического излучения и хроматической дисперсии оптического волокна.

8. Результаты работы внедрены и используются в Казахском национальном исследовательском техническом университете им. К.И. Сатпаева, Национальном

авиационном университете (Киев, Украина), УО «Белорусская государственная академия связи» (Минск, Беларусь) и компании AxxonSoft (Киев, Украина), что подтверждено соответствующими актами внедрения.

Оценка полноты решений поставленных задач

В результате выполнения диссертационных исследований все поставленные задачи решены в полном объеме:

- проведен анализ современных методов, моделей и коммерческих систем распределения ключей шифрования по критериям безопасности (защищенности) и скорости;
- разработаны модель угроз и модель нарушителя в квантово-криптографических системах;
- разработана и исследована модель квантового детерминистического протокола в режиме контроля подслушивания;
- разработана и исследована модель квантового детерминистического протокола в режиме передачи сообщений;
- разработана комбинированная модель с режимом контроля подслушивания и режимом передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов;
- усовершенствован метод безопасного распределения ключей комбинированной модели с режимом контроля подслушивания и режимом передачи сообщений квантового детерминистического протокола.

Рекомендации и исходные данные по конкретному использованию результатов

На основании выполненных исследований рекомендуется:

1) использовать абстрактную модель нарушителя в системах КК для определения совокупности мероприятий различного характера, необходимых для дополнительного внедрения в специфические квантовые системы для обеспечения надежной защиты;

2) использовать генератор троичных псевдослучайных последовательностей, для повышения уровня доступности квантового канала при передаче ключа детерминистическим протоколом и небольшом уровне природных шумов;

3) использовать квантовый детерминистический протокол с парами перепутанных кутритов и предложенный метод усиления секретности для организации безопасного распределения ключей, повышения скорости передачи и обеспечения помехоустойчивости деполяризационного квантового канала Повышение скорости в 22,1 – 36,2 раза (для симметрических криптографических систем с длинной (ключа 128-256 бит) без потерь стойкости детерминистических протоколов квантовой криптографии с использованием пар кутритов устойчивых к некогерентной атаке.

4) полученные статистические данные, подтверждают пригодность троичных кодов Рида –Соломона для коррекции ошибок (при небольшом уровне природных шумов в квантовом канале) и способность обеспечивать высокую доступность квантового канала при реализации типовых протоколов, если вероятность деполяризации кутрита в квантовом канале не превышает 20-25%.

5) для надежного детектирования атаки легитимные пользователи должны использовать квантовый канал с естественным уровнем шумов, на практике это означает использование канала ограниченной длины с естественным уровнем шумов $p \leq 0,7$.

6) результаты исследования были использованы в учебном процессе КазНИТУ имени К.И. Сатпаева, Национального авиационного университета, УО «Белорусская государственная академия связи», компании AxxonSoft, что приведено в актах внедрения результатов исследования (Приложение В).

Оценка научного уровня выполненной работы в сравнении с лучшими достижениями в данной области

Оценка научного уровня выполненной работы в сравнении с лучшими достижениями в данной области проведена на основании анализа научно-технических литературных источников, посвященных тематике «Методы безопасного распределения ключей на базе протоколов квантовой криптографии». Выбор индекса классификации и глубины поиска в разрезе **10** лет, соответствующие теме исследования обеспечивают надежность и достоверность поиска актуальных информационных материалов. В результате проведенного анализа определено, что научный уровень выполненной диссертационной работы обладает достаточной новизной и в целом соответствует мировому техническому уровню и тенденциям развития технологий защиты информации, методам безопасного распределения ключей.

Автор выражает глубокую благодарность всем сотрудникам и профессорско-преподавательскому составу Национального авиационного университета, УО Белорусской государственной академии связи, КазНИТУ имени К.И.Сатпаева за оказанную техническую, консультационную помощь в выполнении экспериментов и анализов, полученных данных настоящей диссертационной работы.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Баричев С.Г., Серов Р.Е. Основы современной криптографии: Учебное пособие. - М.: Горячая линия – Телеком, 2002. - 152 с.

2 Мао В. Современная криптография: теория и практика: пер. с англ. - М.: Вильямс, 2005. - 768 с.

3 Фергюсон Н., Шнайер Б. Практическая криптография. - М.: Вильямс, 2005. - 424 с.

4 Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: пер. с англ. - М.: Вильямс, 2001. - 672 с.

5 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. - 816 с.

6 Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления. /пер. с анг. С.П. Кулик, Е.А. Шапиро; С.П. Кулик, Т.А. Шмаонов (ред. пер.); Д. Боумейстер и др. (ред.). - М.: Постмаркет, 2002. - С. 33–73.

7 Advanced Technologies of Quantum Key Distribution, Monograph. edited by Sergiy Gnatyuk. - London. Great Britain: InTech, 2018. - 227 p. DOI: 10.5772/65232

8 SECOQC White Paper on Quantum Key Distribution and Cryptography //http://www.arxiv.org/abs/quant-ph/0701168v1

9 Korchenko O., Vorobiyenko P., Vasiliu Ye., Gnatyuk S. and others, Quantum secure telecommunication systems, Telecommunications Networks. Current Status and Future Trends. Monograph. Edited by J.H. Ortiz. Rijeka. Croatia: InTech, 2012. –C. 211-236, https://www.intechopen.com/books/telecommunications-networks-current-status-and-future-trends/quantum-secure-telecommunication-systems.

10 Килин С.Я., Хорошко Д.Б., Низовцев А.П. Квантовая криптография: идеи и практика. - Минск: Белорусская наука, 2008. - 392 с.

11 Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. - М.: Мир, 2006. - 824 с.

12 Корченко О.Г., Василіу Є.В., Гнатюк С.О. Сучасні квантові технології захисту інформації. //Захист інформації, - 2010. - № 1. - С. 77–89.

13 Lo H.-K., Zhao Yi. Quantum cryptography. //Encyclopedia of Complexity and Systems Science. – N.Y.: Springer US, - 2009. - Vol. 8. - P. 7265–7289.

14 Корченко О.Г., Луцький М. Г., Гнатюк С.О. Сучасні комерційні системи квантової криптографії. //Сучасна спеціальна техніка, - 2011. - № 4. - С. 37-42.

15 Корченко О.Г., Василіу Є.В., Гнатюк С.О., Кінзерявий В.М. Атаки в квантових системах захисту інформації. //Вісник інженерної академії України, - 2010. - №3-4. - С. 124–133.

16 Cai Q.Y. The «ping-pong» protocol can be attacked without eavesdroppig. //Physical Review Letters, - 2003. - Vol. 91. issue 10. 109801.

17 Bostrom K., Felbinger T. Deterministic secure direct communication using entanglement. //Physical Review Letters, - 2002. - Vol. 89, P. 1-5. issue 18. – 187902.

18 Gnatyuk S., Zhmurko T., Falat P. Efficiency Increasing Metod for Quantum Secure Direct Communication Protocols. //The 8th IEEE International Conference on

Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Warsaw. Poland, 2015. - P. 125-130.

19 Гнатюк С.О., Жмурко Т.О., Кінзерявий В.М., Одарченко Р.С., Абакумова А.О., Стояновіч А.Д. Спосіб підсилення стійкості квантових протоколів прямого безпечного зв'язку, [заявник та патентовласник НАУ]. Пат. №108520 України, МПК H04K 1/06. № u201512445, заявл. 16.12.2015. опубл. 25.07.2016. Бюл. №14, - 5 с.

20 QPN Security Gateway //http://www.magiqtech.com/MagiQ/Products.html

21 Cerberis //http://www.idquantique.com/products/cerberis.html, 01.12.15

22 QKS. Toshiba Research Europe Ltd., Cambridge Research Laboratory //http://www.toshiba-europe.com/research/crl/qig/ quantumkeyserver.html, 01.12.15

23 QUANTIS: True Random Number Generator /http://www.idquantique.com/true-random-number-generator/products-overview.html

24 Жмурко Т.А., Кинзерявый В.Н., Юбузова Х.И., Стоянович А.Д., Узагальнена класифікація методів квантовой криптографіі та зв'язку. //Scientific Journal of Information Security. Ukrainian, - 2015. – Т. 22, issue 3. - P. 287-293. ISSN 2225-5036 (ISSN 2411-071X)

25 Ахметов Б.С., Кинзерявий В.М., Жмурко Т.О., Юбузова Х.И. Розширення номенклатури методів квантовоі криптографіі та звязку. Материалы II международной научно-практической конференции «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації». – Киев: Европейский университет, 2016. – С. 11-14.

26 Шаховал О., Юбузова Х.И. Стратегія кібербезпеки України у контексті інформаційно-психологічного впливу. Матеріали VI міжнародноі науково-технічноі конференціі ITSEC. – Київ: Національный авіаційний університет, 2016. – С. 73.

27 Гнатюк С., Охріменко Т., Юбузова Х. Новітні квантово-криптографічні системи та технології. //Матеріали VIII міжнародної науково-технічної конференції «Інфокомунікації – сучасність та майбутнє». - Одесса, 2018. - С. 85-88

28 Wojcik A. Eavesdropping on the «Ping-Pong» Quantum Communication Protocol. //Physical Review Letters, - 2003. - Vol. 90. issue 15. 157901.

29 Zhang Z.J., Li Y., Man Z.X. Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss. //Physical Letters A, - 2005. - Vol. 341. issues 5–6. - P. 385–389.

30 Deng F.G., Zhou P., Li X.H. et al. Robustness of two-way quantum communication protocols against Trojan horse attack. //http://arxiv.org/abs/quant-ph/0508168

31 Li X.H., Deng F.G., Zhou H.Y. Improving the security of secure direct communication based on the secret transmitting order of particles. //Physical Review A, - 2006. - Vol. 74. issue 5. –054302.

32 Василіу Є.В. Пінг-понг протокол з повністю переплутаними станами пар та триплетів тривимірних квантових систем. //Цифрові технології, - 2009. - № 5. - С. 18–26.

33 Василіу Є. Пінг-понг протокол з повністю переплутаними станами пар та триплетів тривимірних квантових систем. //Матеріали Міжнародної науково-

технічної конференції «Технології цифрового мовлення: стратегія впровадження» (DBT–2009). Одеса: ОНАЗ ім. О.С. Попова, 2009. - С. 254 – 262.

34 Gnatyuk S., Zhmurko T., Kinzeryavyy V., Yubuzova Kh. Security intruder model in quantum cryptography systems. //Інформаційна безпека та комп'ютерні технології. III Міжнародна науково-практична конференція, 19-20 квітня 2018 року. 2018. – С. 19-21.

35 Ostermeyer M., Walenta N. On the implementation of a deterministic secure coding protocol using polarization entangled photons. //Optics Communications, - 2008. - Vol. 281. issue 17. - P. 4540–4544.

36 Василиу Е.В., Мамедов Р.С. Анализ атаки пассивного перехвата на пинг-понг протокол с полностью перепутанными парами кутритов. //Восточноевропейский журнал передовых технологий, - 2009. - № 4/2 (40). - С. 4–11.

37 Юбузова Х.И. Квантовая криптография и принципы работы алгоритма квантового распределения ключей. //Сборник трудов Международного форума «Инженерное образование и наука в XXI веке: Проблемы и перспективы». – Алматы: КазНТУ, 2014. – Т. II. - С. 400-405.

38 Cai Q.Y., Li B.W. Improving the capacity of the Bostrom–Felbinger protocol. //Physical Review A, - 2004. - Vol. 69. issue 5. – 054301.

39 Юбузова Х.И. Квантовый протокол распределения ключей. Сборник трудов II Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика» – Алматы: КазНИТУ им. К.И.Сатпаева, 2015. – Т. II. – С. 377-381.

40 Василиу Е.В. Стойкость пинг-понг протокола с триплетами Гринбергера – Хорна – Цайлингера к атаке с использованием вспомогательных квантовых систем. //Информатика: Объединенный институт проблем информатики НАН Беларуси, - 2009. - № 1 (21). - С. 117–128.

41 Lomonaco S.J., Jr. A. Quick Glance at Quantum Cryptography. //Cryptologia, - 1999. - V. 23. - num. 1. - P. 1–41.

42 Bruss D., Lutkenhaus N. Quantum Key Distribution: from Principles to Practicalities. //Applicable Algebra in Engineering, Communication and Computing, - 2000. - Vol. 10. - num. 4-5. - P. 383–399.

43 Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography. //Review of Modern Physics, - 2002. - Vol. 74. issue 1. - P. 145–195.

44 Scarani V., Bechmann-Pasquinucci H., Cerf N. J. et al. The security of practical quantum key distribution. //Review of Modern Physics, - 2009. - Vol. 81. issue 3. - P. 1301–1350.

45 Lo H.-K., Zhao Yi. Quantum cryptography. //Encyclopedia of Complexity and Systems Science. – N.Y.: Springer US, - 2009. - Vol. 8. - P. 7265–7289.

46 Василиу Е.В., Воробиенко П.П. Проблемы развития и перспективы использования квантово-криптографических систем. //Наукові праці ОНАЗ ім. О.С. Попова, - 2006. - № 1. - С. 3–17.

47 Gnatyuk S., Zhmurko T., Iavich M., Yubuzova Kh. Deterministic Quantum Cryptography Protocol Model for Depolarized Quantum Channel. //Proceedings of

International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMico), - 2018. - P. 23-32.

48 Ahmetov B., Gnatyuk S., Kinzeryavyy V., Yubuzova Kh. Model of simulation of operation of the deterministic protocol of safe communication in the quantum channel with noise. //Bulleten of National Academy of Sciences of the Republic of Kazakhstan, - Алматы, 2018. - Vol. 2. - Number 372. – С. 6 – 16. ISSN 1991-3494

49 Akhmetov B., Gnatyuk S., Zhmurko T., Kinzeryavyy V., Yubuzova Kh. Experimental study of the simulation model for deterministic secure communication protocol in quantum channel with noise. //Reports of the National Academy of sciences of the republic of Kazakhstan, - Алматы, 2018. – Vol. 5. - Number 321. - P. 5-11. ISSN 2518-1483 (Online), ISSN 2224-5227 (Print), doi.org/10.32014/2018.2518-1483.1

50 Gnatyuk S., Kinzeryavyy V., Kyrychenko K., Yubuzova Kh., Aleksander M., Odarchenko R. Secure Hash Function Constructing for Future Communication Systems and Networks. //17th International Conference on Computer Information Systems and Industrial Management Applications, Moscow. 2018. - P. 561-569

51 Akhmetov B., Gnatyuk S., Okhrimenko T., Kinzeryavyy V., Yubuzova Kh., Gancarczyk T., Bernas M. Experimental research of the corrective ability of interference stable Reed-Solomon codes over the *GF* (32) Galois field at transferring information on a deterministic quantum and cryptographic protocol. //Вестник КазНИТУ, - Алматы, 2019. - №2 (132). - P.61-69. ISSN 1680-9211

52 Zhengbing Hu, Gnatyuk S., Zhmurko T., Yubuzova Kh. High-speed privacy amplification method for deterministic quantum cryptography protocols using pairs of entangled qutrits. //CEUR Workshops Proceedings. Vol.2393, - 2019. - P 810-821. ISSN 1613-0073

53 Vaziri A, Weihs G., Zeilinger A. Experimental Two-Photon, Three-Dimensional Entanglement for Quantum Communication. //Physical Review Letters, - 2002. - Vol. 89. issue 24. 240401.

54 Vaziri A., Pan J., Jennewein T. et. al. Concentration of higher dimensional entanglement: qutrits of photon orbital angular momentum. //Physical Review Letters, - 2003. - Vol. 91. issue 22. 227902.

55 Akhmetov B., Gnatyuk S., Zhmurko T., Yubuzova Kh. Simulation model for deterministic protocol of quantum secure direct communication with error-correcting coding. //Вестник КазНИТУ, - Алматы, 2018. - №5 (129). - P. 150-158. ISSN 1680-9211

56 Wang Ch., Deng F.G., Li Y.S. et al. Quantum secure direct communication with high dimension quantum superdense coding. //Physical Review A., - 2005. - Vol. 71. issue 4. 044305.

57 Корченко О.Г., Васіліу Є.В., Гнатюк С.О., Кінзерявий В.М. Імітаційна модель пінг-понг протоколу з парами переплутаних кутритів у квантовому каналі з шумом. //Захист інформації, - 2010. - № 3. - С. 46–56.

58 Ramzan M., Khan S., Khan M.K. Noisy non-transitive quantum games. //J. Phys. A: Math. Theor, - 2010. - Vol. 43, - N. 26. 265304.

59 Блейхут Р. Теория и практика кодов, контролирующих ошибки. - М.: Мир, 1986. - 576 с.

60 Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. - М.: Техносфера, 2005. - 320 с.

61 Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979. - 744 с.

62 Вернер М. Основы кодирования: учебник для ВУЗов. – М.: Техносфера, 2004. – 288 с.

63 Корченко О.Г., Васіліу Є.В., Гнатюк С.О., Кінзерявий В.М. Оцінка коригувальної здатності завадостійких трійкових РС-кодів при передачі інформації повністю переплутаними станами кутритів квантовим каналом із шумом. //Захист інформації, - 2010. - № 4. - С. 44–53.

64 Василиу Е.В., Мильчевич В.Я. и др. Безопасные системы передачи конфиденциальной информации на основе протоколов квантовой криптографии. - Харьков: Цифровая типография № 1, - 2013. – 168 с.

65 Гнатюк С., Жмурко Т., Кінзерявий В., Юбузова Х. Експериментальне дослідження методу забезпечення стійкості кутритових протоколів квантовоі криптографії. //Захист інформації, - 2016. – Т. 18, - №3. – С. 218-228. ISSN 2221-5212

66 Gnatyuk S., Zhmurko T., Yubuzova Kh. Experimental studies of efficiency improving method for quantum cryptography. //Международна научна конференция УНИТЕХ'16. Сборник доклади. – Габрово, 2016. - Т. II. - P. 425-430. ISSN 1313-230X

67 Жмурко Т.О., Поліщук Ю.Я., Юбузова Х. Експериментальне дослідження методу генерування тритових послідовностей. //Актуальні питання забезпечення кібербезпеки та захисту інформації: тези доповідей учасників III Міжнародної науково-практичної конференції (Закарпатська область, Міжгірський район, село Верхнє Студене, туристичний комплекс «Едельвейс»). - К.: Видавництво Європейського університету, 2017. – С. 76-80.

68 Gnatyuk S., Zhmurko T., Yubuzova K. Privacy amplification method for deterministic quantum cryptography protocols. //Актуальні питання забезпечення кібербезпеки та захисту інформації: тези доповідей учасників IV Міжнародної науково-практичної конференції Закарпатська область, Міжгірський район, село Верхнє Студене, туристичний комплекс «Едельвейс». - К.: Видавництво Європейського університету, 2018. – С. 129-132.

69 Gnatyuk S., Kinzeryavyy V., Iavich M., Prysiazhnyi D., Yubuzova Kh. High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks. //Proceedings of the 14th Intern. Conf. on ICT in Education. Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Vol. II: Workshops. Kyiv: Ukraine, May 14-17. - 2018. - P. 657-668.

70 Сушко С.О., Кузнецов Г.В., Фомичова Л.Я., Корабльов А.В. Математичні основи криптоаналізу: Навч. посібник - Д.: Національний гірничий університет, 2010. - 465 с.

71 Гнатюк С.О., Жмурко Т.О., Кінзерявий В. М, Сєйлова Н. А. Метод генерування тритових псевдовипадкових послідовностей для систем квантової криптографії. //Безпека інформації, - 2015. - № 2 (22). - С. 140-147.

72 Василиу Е.В., Николаенко С.В. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений. //Наукові праці ОНАЗ ім. О.С. Попова, - 2009. - № 1. - С. 83–91.

73 Василиу Е.В. Оценки вычислительной сложности неквантового способа усиления безопасности пинг-понг протокола. //Прикладная радиоэлектроника, - 2009. - № 3. - С. 396–404.

74 Гнатюк С.А., Жмурко Т.А., Кинзерявий В.Н., Юбузова Х.И. Статистическое тестирование псевдослучайных троичных последовательностей для применения в тритовых протоколах квантовой криптографии. //Материалы международной научной конференции «Современные средства связи». – Минск: УО Белорусская государственная академия связи, 2018. - С. 206-208.

75 Шелест. М.Є., Гнатюк С.О., Жмурко Т.О., Кінзерявий В.М., Юбузова Х.І. Експериментальне дослідження методу генерування тритових псевдовипадкових послідовностей для криптографічних застосувань. //Захист інформації, - 2017. - Т. 19. - № 1. - С. 67-79. DOI: 10.18372/2410-7840.19.11478**.** ISSN 2410-7840 (Online). ISSN 2221-5212 (Print)

76 Гнатюк С., Жмурко Т., Кінзерявий В., Сєйлова Н. Метод оцінювання якості тритових псевдовипадкових послідовностей для криптографічних застосувань. //Information Technology & Security, - 2015. - V. 3. Issue 2. - С. 108-116.

77 Gnatyuk S. Comparative Analysis of Quantum Key Distribution Systems. //Science-Based Technologies, - 2013. - №1. – P. 68-72.

78 Рудницкий В.Н., Корченко А.Г., Гнатюк С.А. Квантовая безопасная прямая связь как метод повышения уровня конфиденциальности информационно-коммуникационных систем. //Системи управління, навігації та зв'язку, - 2011. - Вип.2 (18). – С. 294-296.

79 Рудницкий В.Н., Корченко А.Г., Гнатюк С.А. Особенности использования современных квантовых технологий для обеспечения конфиденциальной связи систем. //Збірник наукових праць Харківського університету Повітряних Сил, – Харків: ХУПС, - 2011. - Вип.2 (28). – С. 80-83.

80 Ye. Vasiliu, S. Gnatyuk, S. Nikolaenko, T. Zhmurko. Security Amplification of the Ping-Pong Protocol with Many-Qubit Greenberger-Horne-Zeilinger States. //Ukrainian Scientific Journal of Information Security, - 2012. - Vol.18. Issue 2. - P. 84-88.

81 Gnatyuk S.O., Okhrimenko T.O (Zhmurko), Akhmetov B.S., Seilova N.A., Yubuzova Kh.I. Approach to Increase Speed for Deterministic Protocols of Quantum Cryptography. «The Eighth World Congress «Aviation in the XXI-st century – Safety in Aviation and Space Technologies». Kyiv, 2018. - P. 302-310.

82 Gnatyuk S., Kinzeryavyy V., Kyrychenko K., Yubuzova Kh., Aleksander M., Odarchenko R. Secure Hash Function Constructing for Future Communication Systems and Networks. //Advances in Intelligent Systems and Computing. - 2020. - P.561-569. DOI: 10.1007/978-3-030-12082-5_51, SPRINGER, ISSN: 2194-5357, ISBN: 9783030120818

83 Akhmetov B., Gnatyuk S., Okhrimenko T., Kinzeryavyy V., Yubuzova Kh. Experimental research of the corrective ability of interference stable Reed-Solomon

codes over the GF(3^2) Galois field at transferring information on a deterministic quantum and cryptographic protocol. //VESTNIK KazNRTU. №2 (132). - Алматы, 2019. - P.61-69. ISSN 1680-9211

84 Akhmetov B., Gnatyuk S., Kinzeryavyy V., Yubuzova Kh. Studies on practical cryptographic security analysis for block ciphers with random substitutions, International Journal of Computing, 19(2), - 2020, P. 298-308. Print ISSN 1727-6209**,** On-line ISSN 2312-5381

85 Rodinko M., Oliynykov R., Yubuzova Kh. Differential cryptanalysis of the lightweight block cipher cypress-256. International Journal of Computing, 19(2), - 2020, P. 273-281. Print ISSN 1727-6209, On-line ISSN 2312-5381

86 Зеневич А.О. Обнаружение утечки информации из оптического волокна. - Минск: Белорусская государственная академия связи, 2017. - 144 с. ISBN 978-985-585-020-6.

87 Гулаков И.Р., Зеневич А.О. Фотоприемники квантовых систем. - Минск: ВГКС, 2012. - 276 с. ISBN 978-985-7002-58-0.

88 Асаенок М.А., Горбадей О.Ю., Зеневич А.О. Коэффициент усиления кремниевого фотоэлектронного умножителя с низким напряжением питания. // Проблемы инфокоммуникаций, - 2017. - № 2 (6). – С. 82-87.

89 Зеневич А.О. Обнаружение несанкционированного доступа при передаче данных по волоконно-оптическим линиям связи. //Веснік сувязі, - 2014. - №5(127). - С. 33-37.

90 Гулаков И.Р., Зеневич А.О. и др. Исследование скорости передачи информации по оптическому каналу связи с приемником на основе счетчиков фотонов. //Автометрия, - 2011. - Т.47. - №4. - С. 31-40.

91 Зеневич А.О. Исследование пропускной способности оптического канала связи, в котором для детектирования сигнала используется счетчик фотонов. //Доклады БГУИР, - 2011. - № 7(61). - С. 5-9.

92 Документация по оборудованию Института информационных технологий. Руководство по эксплуатации. Оптического тестера ОТ-2-8, рефлектометра МТР 600, мобильной измерительной платформы МТР 9000А, измерителя хроматической дисперсии ИД-2-2/12.

93 Юбузова Х.И. Методы защиты информации от съема в ВОЛС. //Сборник трудов Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика». -Алматы, КазНТУ, 2012. - Т. 2. - С.459-463, ISBN 978-601-228-396-9; ISBN 978-601-228-394-5

94 Юбузова Х.И., Оган А. Проблемы защиты информации в волоконно-оптических линиях связи от несанкционированного доступа. //Сборник трудов Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика». - Алматы, КазНТУ, 2012. - Т. 2. - С. 463-466, ISBN 978-601-228-396-9, ISBN 978-601-228-394-5

95 Юбузова Х.И., Кабдулгазыев А.Н., Сартаев Б.С. Каналы утечки информации и способы защиты в оптических линиях связи. //Сборник Международной

научно-практической конференции «Подготовка инженерных кадров в контексте глобальных вызовов XXI века», секция «Новые информационные и телекоммуникационные технологии, технологии создания интеллектуальных систем», 3 том. -Алматы, КазНТУ, 2013. - С. 49-52, ISBN 978-601-228-568-0

96 Юбузова Х.И. Методы компенсации дисперсии. //Поиск. Научный журнал министерства образования и науки РК, - Алматы, 2013. - № 2 (2). - С. 236-241, ISNN 1560-1730

97 Юбузова Х.И., Бакытжанов Б.К. Особенности обеспечения безопасности в оптоволоконных кабельных системах. //Сборник трудов Международных Сатпаевских чтений «Роль и место молодых учены в реализации стратегии «Казахстан-2050». -Алматы, КазНТУ, 2014. - Т.3. - С. 226-231, ISBN 978-601-228-657-1; (ISBN 978-601-228-660-1).

98 Gnatyuk S., Hu Zh., Sydorenko V., Aleksander M., Polishchuk Y., Yubuzova Kh. Cases on Modern Computer Systems in Aviation. /Critical Aviation Information Systems: Identification and Protection. Monograph. IGI Global, 2019. – P. 423-448. ISBN13: 9781522575887, DOI: 10.4018/978-1-5225-7588-7. ch17, https://www.igi-global.com/chapter/critical-aviation-information-systems/222199

99 Холево А.С. Введение в квантовую теорию информации. –М.: МЦНМО, 2002. – 128 с.

100 Имре Ш., БаллажФ. Квантовые вычисления и связь. Инженерный подход. –М.: Физматлит, 2008. – 320 с.

101 Гнатюк С., Охріменко Т., Юбузова Х. Новітні квантово-криптографічні системи та технології. //Матеріали IIV Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації». - Киев Видавництво Європейського університет, 2021. – С. 144-147

102 Дорожинський С.А., Охріменко Т.О., Юбузова Х.И., Жаксигулова Д.Д. Інтегрування квантово-криптографічних технологій в сучасні комункаційні системи та мережі. //Матеріали VII Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації». 2021. - С.30-34

103 Gnatyuk S., Ryabyi M., Dorozhynskyi S., Yubuzova K. About the combination of quantum key distribution and lightweight cryptography for data privacy. //Abstracts of the IVth International scientific-practical conference dedicated to the 50th anniversary of the Department of Information Systems and Technologies. Integration of information systems and intelligent technologies in the conditions of information society transformation. 2021. Полтава. P. 82-86. ISBN 978-966-289-562-9, DOI: https://doi.org/10.32782/978-966-289-562-9

ПРИЛОЖЕНИЕ А

Листинг программы для моделирования квантового детерминистического протокола в режиме контроля подслушивания

```
%%% ПРОТОКОЛ С ПАРАМИ <<<КУТРИТОВ>>> И СВЕРХПЛОТНЫМ
%%% КОДИРОВАНИЕМ В КАНАЛЕ С ШУМОМ
%%%                    (ДЕПОЛЯРИЗУЮЩИЙ КАНАЛ)
classdef DPK_3_ver_1_1_for_GUI

   properties
      kk;
      q_RezumivPeremukannya;
      length2;
      Rozmir;
      Nat_chan_err_lev;
      block_quantity;
      kol_err_received;

      Dx;
      Dz;
      D_Eva;

      Err_x;
      Err_z;
      Err_mean;

      Min_error_level;
      Max_error_level;
      Mean_error_level;

      Min_error_level_x;
      Max_error_level_x;
      Mean_error_level_x;

      Min_error_level_z;
      Max_error_level_z;
      Mean_error_level_z;

      I0_x;
      I0_z;
      I0;
   end

   methods
      %%%
##########################################################################
############
      %%%
##########################################################################
############
```

```
        %%% konstryktor
        function Obj = DPK_3_ver_1_1_for_GUI(length_, kk_, q_, Dx_, p_)
            %%% length - длина передаваемых данных
            %%
            %%
            Obj.length2 = length_;

            %%% kk - показатель степени десятки для вероятности
            %%% необнаружения атаки, т.е. s = 10^(-kk).
            Obj.kk = kk_;

            %%% q - вероятность переключения
            %%% протокола в режим контроля подслушивания.
            %%% 1 - q - вероятность переключения
            %%% протокола в режим контроля передачи сообщения
            Obj.q_RezumivPeremukannya = q_;

            %%% Dx - вероятность обнаружения атаки в базисе X
            Obj.Dx = Dx_;

            %%% p - вероятность получения ошибки
            %%% в канале связи
            Obj.Nat_chan_err_lev = p_;

            %%% запускаем модель детерминистического протокола с определенными парамет-
рами
            Obj = DPK_3_Noise_chan_ver_3_1_(Obj);

        end
        %%%
########################################################################################
############
        %%%
########################################################################################
############
    end

    methods
        %%%
########################################################################################
############
        %%%
########################################################################################
############
        %%% DPK_3_Noise_chan_ver_3_0
        function Obj = DPK_3_Noise_chan_ver_3_1_(Obj)


            %%%%#################################################################
            %%%
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
            %%% Этап 0. Расчет длины блока для протокола с парой кутритов и расчет D_Eva
```

```
        %%% kk - показатель степени десятки для вероятности не обнаружения атаки,
        %%% т.е. s = 10^(-kk)

        %%% считаем для надежности, что E получает полную информацию за один раунд,
        %%% т.е. 2 трита, что увеличит длину блока

        %%% также считаем, что E создает минимальный уровень ошибок d = <<<1/3>>>,
        %%% при этом длина блока будет максимальна по d

        %%% пусть Dz = <<<2/3>>> всегда; Dx задаем, как параметр
        Obj.Dz = 2/3;

        %%% вероятности выбора базисов (Q_bas_z, Q_bas_x) для контроля подслушива-
ния
        %%% пока задаем явно по 0.5 (наиболее разумная стратегия для A & B)
        Q_bas_z = 0.5;
        Q_bas_x = 1 - Q_bas_z;
        Obj.D_Eva   = Q_bas_z * Obj.Dz + Q_bas_x * Obj.Dx;

        INF     = -Obj.kk * 2 / log10((1 - Obj.q_RezumivPeremukannya) / (1 - Obj.q_Re-
zumivPeremukannya * (1 - 1 / 3)));

        %%% вычисляем длину блока
        Rozm    = ceil(INF);
        if (mod(Rozm, 2) == 0)
           Obj.Rozmir = Rozm;
        else
           Obj.Rozmir = Rozm + 1;
        end

        %%% МОДЕЛЬ ШУМА В ДЕПОЛЯРИЗУЮЩЕМ КАНАЛЕ!
        Obj.Err_x       = Obj.Dx + (3/4) * Obj.Nat_chan_err_lev * (1 - (3/2) * Obj.Dx);
        Obj.Err_z       = Obj.Dz + (3/4) * Obj.Nat_chan_err_lev * (1 - (3/2) * Obj.Dz);
        Obj.Err_mean    = Q_bas_z * Obj.Err_z + Q_bas_x * Obj.Err_x;

      %%%%#########################################################################


      %%%%#########################################################################
      %%%
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      %%% Этап 1. Получение исходной битовой строки сообщения

        %%% поскольку нужно из длины данных length сделать блоки
        %%% длиной Rozmir, определим количество вспомогательных символов,
        %%% которые добавим, чтобы длина length была кратна Rozmir
        ost     = rem(Obj.length2, Obj.Rozmir);

          %%% вероятности комбинаций 00, 01, 02, 10, 11, 12, 20, 21, 22.
          p00 = 1 / 9;
          p01 = 1 / 9;
          p02 = 1 / 9;
```

```
        p10 = 1 / 9;
        p11 = 1 / 9;
        p12 = 1 / 9;
        p20 = 1 / 9;
        p21 = 1 / 9;
        p22 = 1 / 9;

      %%% сюда можно будет вставлять тритовые строки,
      %%% пока генерируем случайную строку
      Text    = fix(3 * rand(1, Obj.length2 + (Obj.Rozmir - ost), 'single'));

      %%% вычисляем кол-во блоков
      Obj.block_quantity = ceil(Obj.length2 / Obj.Rozmir);
    %%%%#########################################################################



%%%%+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      %%% ОТКРЫВАЕМ ЦИКЛ ПО БЛОКАМ
      kkk = 1;
      Obj.kol_err_received = 0;

      for ttt = 1 : Obj.block_quantity

        %%% разбиваем строку на блоки
        for j = 1 : Obj.Rozmir
          Block(j) = Text(kkk);
          kkk = kkk + 1;
        end
        Block_tr = Block';
```

ПРИЛОЖЕНИЕ Б

Листинг программы для моделирования квантового детерминистического протокола в режиме передачи сообщений

```
%%% ПРОТОКОЛ С ПАРАМИ <<<KYTRITOV>>> И СВЕРХПЛОТНЫМ КОДИРОВА-
НИЕМ В КАНАЛЕ С ШУМОМ (ДЕПОЛЯРИЗУЮЩИЙ КАНАЛ)
%%% С ПОМЕХОУСТОЙЧИВЫМ КОДОМ РИДА_СОЛОМОНА

classdef DPK_3_ver_2_1_for_GUI

    %%% параметры детерминистического протокола +++
    properties
        kk;
        q_RezumivPeremukannya;
        length;
        Rozmir;
        Nat_chan_err_lev;
        block_quantity;
        kol_err_received;

        Dx;
        Dz;
        D_Eva;

        %%% <<<Вспомогательные таблицы для работы в поле GF(3)>>>
        Matrica_Dodavannya  = [0, 1, 2; 1, 2, 0; 2, 0, 1];
        Matrica_Vidnimannya = [0, 2, 1; 1, 0, 2; 2, 1, 0];
        Matrica_Mnozennya   = [0, 0, 0; 0, 1, 2; 0, 2, 1];
        Matrica_Dilennya    = [0, 0, 0; 0, 1, 2; 0, 2, 1];
    end

    %%% параметры для RS-koda +++
    properties

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        %%% выставляем начальные параметры:
        %%% N = q - 1, а q = 3^2, N – количество всего слов в GF(9)
        %%% s = 2, s – длина слова, слово отображено в GF(3)
        %%% k – количество информационных слов, выбираем случайно. Можно уменьшить!
        %%% r = количество дополнительных слов
        %%% D – min растояние из всех расстояний Хемминга
        %%% tt – количество символов, которые можно исправить! Округлено в меньшую
        %%% сторону +++
            N = 8;
            K = 4;
            %r = N - K;
            r = 4;
            %D = r + 1;
            D = 5;
```

```
    %tt = floor(r / 2);
    tt = 2;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    %%% поле GF(9) построим по полиному x^2 + x + 2,  и отобразим его над
    %%% полем GF(3):
    %%%    0 = (0 0) =      0  = 0
    %%%    1 = (0 1) =      1  = a^8
    %%%    2 = (0 2) =      2  = a^4
    %%%    3 = (1 0) = x       = a
    %%%    4 = (1 1) = x  + 1  = a^7
    %%%    5 = (1 2) = x  + 2  = a^6
    %%%    6 = (2 0) = 2x      = a^5
    %%%    7 = (2 1) = 2x + 1  = a^2
    %%%    8 = (2 2) = 2x + 2  = a^3

    %%% представим пару (x, y) в виде числа по gf(9) +++
     Alf_GF9        = [ 0,  1,  2;
                   3,  4,  5;
                   6,  7,  8 ];

     Alf_GF3        = [ 0, 0;
                   0, 1;
                   0, 2;
                   1, 0;
                   1, 1;
                   1, 2;
                   2, 0;
                   2, 1;
                   2, 2 ];

     Alf_GF3_bez00    = [ 0, 1;
                   0, 2;
                   1, 0;
                   1, 1;
                   1, 2;
                   2, 0;
                   2, 1;
                   2, 2 ];

    %%% Вспомогательные таблицы для работы в поле GF(9) построим на полиноме
%%%   x^2 + x + 2
     Matr_Slozeniya_GF9     = [ 0, 1, 2,  3, 4, 5,  6, 7, 8;
                      1, 2, 0,  4, 5, 3,  7, 8, 6;
                      2, 0, 1,  5, 3, 4,  8, 6, 7;
                      3, 4, 5,  6, 7, 8,  0, 1, 2;
                      4, 5, 3,  7, 8, 6,  1, 2, 0;
                      5, 3, 4,  8, 6, 7,  2, 0, 1;
```

```
                        6, 7, 8,  0, 1, 2,  3, 4, 5;
                        7, 8, 6,  1, 2, 0,  4, 5, 3;
                        8, 6, 7,  2, 0, 1,  5, 3, 4 ];

    Matr_Otrizaniya_GF9   = [ 0, 2, 1,  6, 8, 7,  3, 5, 4;
                        1, 0, 2,  7, 6, 8,  4, 3, 5;
                        2, 1, 0,  8, 7, 6,  5, 4, 3;

                        3, 5, 4,  0, 2, 1,  6, 8, 7;
                        4, 3, 5,  1, 0, 2,  7, 6, 8;
                        5, 4, 3,  2, 1, 0,  8, 7, 6;

                        6, 8, 7,  3, 5, 4,  0, 2, 1;
                        7, 6, 8,  4, 3, 5,  1, 0, 2;
                        8, 7, 6,  5, 4, 3,  2, 1, 0 ];

    Matr_Ymnozeniya_GF9   = [ 0, 0, 0,  0, 0, 0,  0, 0, 0;
                        0, 1, 2,  3, 4, 5,  6, 7, 8;
                        0, 2, 1,  6, 8, 7,  3, 5, 4;

                        0, 3, 6,  7, 1, 4,  5, 8, 2;
                        0, 4, 8,  1, 5, 6,  2, 3, 7;
                        0, 5, 7,  4, 6, 2,  8, 1, 3;

                        0, 6, 3,  5, 2, 8,  7, 4, 1;
                        0, 7, 5,  8, 3, 1,  4, 2, 6;
                        0, 8, 4,  2, 7, 3,  1, 6, 5 ];

    Matr_Deleniya_GF9     = [ 0, 0, 0,  0, 0, 0,  0, 0, 0;
                        0, 1, 2,  4, 3, 7,  8, 5, 6;
                        0, 2, 1,  8, 6, 5,  4, 7, 3;

                        0, 3, 6,  1, 7, 8,  2, 4, 5;
                        0, 4, 8,  5, 1, 3,  7, 6, 2;
                        0, 5, 7,  6, 4, 1,  3, 2, 8;

                        0, 6, 3,  2, 5, 4,  1, 8, 7;
                        0, 7, 5,  3, 8, 2,  6, 1, 4;
                        0, 8, 4,  7, 2, 6,  5, 3, 1; ];

    %%% g(x) – порождающий многочлен, g(x) = (x - a)(x - a^2)(x - a^3)(x - a^4) =
    %%% = x^4 + a^7x^3 + a^2x^2 + a^4x + a^2 +++
      g_x = [ 1, 4, 7, 2, 7]

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

    Iskazeniu     = 0;
    Isp_iskazeniu  = 0;
    KolPovtornoPeredavaemuhPodBlokov = 0;
  end
```

```
    %%% конструктор +++
    methods
        %%%
##########################################################################
############
        %%%
##########################################################################
############
        function Obj = DPK_3_ver_2_1_for_GUI(length_, kk_, q_, Dx_, p_)

            %%% length - длина передаваемых данных
            Obj.length = length_;

            %%% kk - показатель степени десятки для вероятности
            %%% не обнаружения атаки, т.е. s = 10^(-kk).
            Obj.kk = kk_;

            %%% q - вероятность переключения
            %%% протокола в режим контроля подслушивания.
            %%% 1 - q - вероятность переключения
            %%% протокола в режим контроля передачи сообщения
            Obj.q_RezumivPeremukannya = q_;

            %%% Dx - вероятность обнаружения атаки в базисе X
            Obj.Dx = Dx_;

            %%% p - вероятность получения ошибки
            %%% в канале связи
            Obj.Nat_chan_err_lev = p_;

            %%% запускаем модель детерминистического протокола с
            %%% определенными параметрами
            Obj = DPK_3_Noise_chan_ver_3_3_for_GUI(Obj);

        end
        %%%
##########################################################################
############
        %%%
##########################################################################
############
    end

    %%% DPK_3_Noise_chan_ver_3_3 +--
    methods
        %%%
##########################################################################
############
        %%%
##########################################################################
############
        function Obj = DPK_3_Noise_chan_ver_3_3_for_GUI(Obj)
```

```
        %%%%#########################################################################
        %%%
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
        %%% Этап 0. Расчет длины блока для протокола с парой
        %%% <<<КУТРИТОВ>>> и расчет D_Eva

            %%% kk - показатель степени десятки для вероятности не обнаружения атаки,
            %%% т.е. s = 10^(-kk)

            %%% считаем для надежности, что E получает полную информацию за один раунд
- 2 <<<трита>>>,
            %%% что увеличит длину блока

            %%% также считаем, что E создает минимальный уровень ошибок d = <<<1/3>>>,
            %%% при этом длина блока будет максимальна по d

            %%% пусть Dz = <<<2/3>>> всегда; Dx задаем, как параметр
            Obj.Dz = 2 / 3;

            %%% вероятности выбора базисов (Q_bas_z, Q_bas_x) для контроля подслушива-
ния
            %%% пока задаем явно по 0.5 (наиболее разумная стратегия для A & B)
            Q_bas_z = 0.5;
            Q_bas_x = 1 - Q_bas_z;
            Obj.D_Eva   = Q_bas_z * Obj.Dz + Q_bas_x * Obj.Dx;

            INF     = -Obj.kk * 2 / log10((1 - Obj.q_RezumivPeremukannya) / (1 - Obj.q_Re-
zumivPeremukannya * (1 - 1 / 3)));

            %%%%% вычисляем длину блока, Rozm – должен делить на 8 -
            %%%%% необходимо для RS-кода
            Rozm    = ceil(INF);
            ost = rem(Rozm, 8);
            if ost == 0
               ost = 8;
            end
            Obj.Rozmir  = Rozm + (8 - ost);
        %%%%#########################################################################


        %%%%#########################################################################
        %%%
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
        %%% Этап 1. Получение исходной битовой строки сообщения
            %%% поскольку нужно из длины данных length сделать блоки
            %%% длиной Rozmir, определим количество вспомогательных символов
            %%% которые добавим, чтобы длина length была кратна Rozmir
            ost     = rem(Obj.length, Obj.Rozmir);
            if ost == 0
               ost = Obj.Rozmir;
            end
```

```
        %%% сюда можно будет вставлять битовые строки файлов, пока генерируем
        %%% случайную строку
        Text    = fix(3 * rand(1, Obj.length +(Obj.Rozmir - ost), 'single'));

        %%% вычисляем кол-во блоков
        Obj.block_quantity = ceil(Obj.length / Obj.Rozmir);
      %%%%#########################################################################


%%%%+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      %%% ОТКРЫВАЕМ ЦИКЛ ПО БЛОКАМ
        kkk = 1;
        Obj.kol_err_received = 0;

        for ttt = 1 : Obj.block_quantity

          %%% разбиваем строку на блоки
          for j = 1 : Obj.Rozmir
            Block(j) = Text(kkk);
            kkk = kkk + 1;
          end
          Block_tr = Block';


%%%%#########################################################################

%%%%++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+
          %%%% Этап 2. Генерация ПСЧП
            PSP = fix(3 * rand(1, Obj.Rozmir, 'single'));
            PSP_tr = PSP';

%%%%#########################################################################

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
          %%%% Этап 3. Сложение
            Izm_Block_tr = rem(PSP_tr + Block_tr, 3);

%%%%%#########################################################################


%%%%#########################################################################
          %%%%
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
          %%%% Этап 4.  Кодирование RS-кодами
            ppp = 0;
            for iii = 1 : (Obj.Rozmir / 8)
              Izm_pod_Block_tr = Izm_Block_tr((ppp + 1) : (ppp + 8));
              POd_Block_RScode = RS_Code(Obj, Izm_pod_Block_tr);
              for jjj = 1 : 16
                  Izm_Text_tr_RScode(2 * ppp + jjj) = POd_Block_RScode(jjj);
```

```
            end
            ppp = ppp + 8;
          end

%%%%%#########################################################################


%%%%#########################################################################
          %%%
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
          %%% Этап 5. Начало протокола. Генерация гаммы для
          %%% переключения режимов передачи сообщения и контроля подслушивания
          %%% Проходим по гамме режимов переключения - пока не передадим
          %%% весь текст.

          %%% В режиме передачи получаем текст и декодируем
          %%% В режиме контроля подслушивания ничего не
          %%% проверяем.

            %%% Вводим новые переменные
            S4et_Rez_Pereda4i_texta       = 0;
            S4et_Rez_Kontrolya_pidslyh    = 0;

            Kil_Podbloka_received         = 0;
            Kil_iskaz_v_Blozi             = 0;
            Izm_PodBlock_received_RScode  = zeros(1, 16);
            Izm_PodBlock_tr_received_RScode = Izm_PodBlock_received_RScode';

            Kil_Teksta_received           = 0;
            Izm_Text_received             = zeros(1, Obj.Rozmir);
            Izm_Text_tr_received          = Izm_Text_received';

            while (1)
              GammaRezumivPeremukannya = rand;

              if(GammaRezumivPeremukannya <= Obj.q_RezumivPeremukannya)
                % контроль подслушивания - в этой модели
                % тут ничего не происходит

                S4et_Rez_Kontrolya_pidslyh          = S4et_Rez_Kontrolya_pidslyh + 1;

              else
                % передача сообщения

                S4et_Rez_Pereda4i_texta       = S4et_Rez_Pereda4i_texta + 1;

                if(Kil_Podbloka_received == 16)
```

ПРИЛОЖЕНИЕ В

Акты внедрения результатов диссертационной работы

УТВЕРЖДАЮ
Проректор по науке
КазНИТУ имени К.И.Сатпаева
_____ Кенжалиев Б.К.
«___» _____ 2018 г

АКТ ВНЕДРЕНИЯ (ИСПОЛЬЗОВАНИЯ)
результатов НИР в учебный процесс

Мы, нижеподписавшиеся, директор института Умаров Т.Ф., заведующий кафедрой Сейлова Н.А. составили настоящий АКТ ВНЕДРЕНИЯ (ИСПОЛЬЗОВАНИЯ) результатов НИР докторанта Специальности 6D070400 «Вычислительная техника и программное обеспечение» Юбузовой Х.И. на тему «Методы безопасного распределения ключей на базе протоколов квантовой криптографии» в учебный процесс для подготовки обучающихся (бакалавриата) по специальности СИБ в виде:

- лекционного курса: Технологии защиты компьютерной информации, Тема «Криптография с секретным и открытым ключом»;
- лабораторных занятий: Технологии защиты компьютерной информации, Тема «Шифрование информации с использованием ассиметричных алгоритмов».

Эффект от внедрения (использования) результатов НИР:

1) обучение студентов бакалавриата новым технологиям защиты и безопасности информации;

2) повышение качества обучения студентов бакалавриата в области информационной безопасности.

Директор Института
Информационных и телекоммуникационных
технологий _____ (подпись) **Умаров Т.Ф.**

Заведующая кафедрой
«Информационная безопасность» _____ (подпись) **Н.А. Сейлова**

УТВЕРЖДАЮ:

Проректор по научной работе Национального авиационного университета

_____ В. Харченко

«05» 09 2018 г.

АКТ

Внедрения результатов диссертационной работы Юбузовой Халичи Ибрагимовны «Методы безопасного распределения ключей на базе протоколов квантовой криптографии» (научные консультанты д.т.н., проф. Ахметов Б.С., д.т.н., доц. Гнатюк С.А.) на соискание ученой степени доктора философии (PhD).

Комиссия в составе: председатель – старший научный сотрудник, к.т.н. Охрименко (Жмурко) Т.А. (ответственный исполнитель), члены – научный сотрудник, к.т.н. Кинзерявый В.Н., младший научный сотрудник, к.т.н. Сидоренко В.Н. составили данный акт о том, что следующие результаты работы Юбузовой Х.И. внедрены и используются в научно-исследовательской работе «Квантово-криптографические методы защиты критической информационной инфраструктуры государства» № 161-ДБ17 (номер госрегистрации 0117U006770):

- модель квантового детерминистического протокола в режиме контроля подслушивания, которая учитывает особенности квантового канала и вероятности возникновения в нем ошибки в *x*- и *z*- базисах измерения, энтропию фон Неймана, а также использует новую процедуру усиления секретности, что позволяет обеспечить безопасное и быстрое распределение ключей (в контексте реализации некогерентной атаки), а также сформулировать практические рекомендации по разработке квантово-криптографических систем в условиях использования деполяризационного квантового канала и присутствия нарушителя;

- модель квантового детерминистического протокола в режиме передачи сообщений, которая за счет формализации системы помехоустойчивого кодирования над полем Галуа $GF(3^2)$ для кутритов, повышения асимптотической стойкости оригинального детерминистического протокола, а также использования алгоритма генерирования троичных псевдослучайных последовательностей, дает возможность повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом и небольшом уровне природных шумов;

- метод усиления секретности, который за счет обработки классической информации перед ее передачей с помощью квантовых перепутанных состояний и использования сгенерированных троичных псевдослучайных последовательностей вместо ресурсоемкого генерирования обратимых матриц над полем Галуа $GF(3^2)$, позволяет повысить скорость без потерь стойкости детерминистических протоколов квантовой криптографии с использованием пар кутритов к некогерентной атаке.

Программная реализация выполнялась на языке программирования C++ в среде разработки Microsoft Visual Studio 2013 (Release версия), а также с использованием специализированных пакетов Wolfram Mathematica 7 и MATLAB 7.

Председатель комиссии,
Старший научный сотрудник, к.т.н. Т. Охрименко (Жмурко)

Члены комиссии:
Научный сотрудник, к.т.н. В. Кинзерявый

Младший научный сотрудник , к.т.н. В. Сидоренко

УТВЕРЖДАЮ
Проректор по научной работе
УО «Белорусская государственная академия связи»

_____ В. В. Дубровский
«2» ноября 2018 г.

АКТ ВНЕДРЕНИЯ

результатов диссертационной работы Юбузовой Халичи Ибрагимовны «Методы безопасного распределения ключей на базе протоколов квантовой криптографии» на соискание ученой степени доктора философии (PhD) в учебный процесс УО «Белорусская государственная академия связи»

Комиссия в составе: председатель – декан факультета электросвязи, канд. техн. наук, доцент Лапцевич А. А.; профессор кафедры инфокоммуникационных технологий, д-р физ.-мат. наук, профессор Гречихин Л. И.; декан факультета инжиниринга и технологий связи, канд. техн. наук, доцент Будник А. В.; заведующий кафедрой математики и физики, канд. техн. наук, доцент Павлюковец С. А. составили настоящий акт о том, что результаты диссертационной работы Юбузовой Халичи Ибрагимовны «Методы безопасного распределения ключей на базе протоколов квантовой криптографии» в 2018/2019 учебном году внедрены в учебный процесс УО «Белорусская государственная академия связи» и используются на кафедре инфокоммуникационных технологий при преподавании дисциплин «Квантовые системы для обеспечения информационной безопасности», «Алгоритмы и методы защиты информации в системах цифровой связи»:

№ п/п	Название внедряемой темы	Форма внедрения	Дисциплина	Эффективность внедрения
1	Современные методы распределения ключей на базе протоколов квантовой криптографии	лекция	Квантовые системы для обеспечения информационной безопасности	Изучение студентами особенностей реализации современных методов распределения ключей шифрования на базе протоколов квантовой криптографии с поляризационным, фазовым и временным кодированием

2	Детерминистический протокол квантовой криптографии с использованием пар перепутанных кутритов	лекция	Квантовые системы для обеспечения информационной безопасности	Ознакомление студентов с режимами работы (контроля подслушивания и передачи сообщений) и особенностями реализации детерминистического протокола квантовой криптографии с использованием пар перепутанных кутритов
3	Система помехоустойчивого кодирования над полем $GF(3^2)$	лекция	Алгоритмы и методы защиты информации в системах цифровой связи	Изучение студентами особенностей и эффективности системы помехоустойчивого кодирования над полем Галуа $GF(3^2)$ для кутритов и их использования в квантовом деполяризационном канале (с шумом)

Председатель комиссии:
декан факультета электросвязи
УО «Белорусская государственная академия связи»
канд. техн, доцент — А. А. Лапцевич

Члены комиссии:
профессор кафедры инфокоммуникационных технологий
д-р физ.-мат. наук, профессор — Л. И. Гречихин

декан факультета инжиниринга и технологий связи
канд. техн. наук, доцент — А. В. Будник

заведующий кафедрой математики и физики
канд. техн. наук, доцент — С. А. Павлюковец

Товариство з обмеженою відповідальністю
«АКССОНСОФТ»
03115, Україна, м. Київ, вул. Львівська, буд. 22-А, офіс - 145
Код ЄДРПОУ-38507216 , тел. +380444821991/фак. +380444093034
П/Р 26009394373 в АТ «РАЙФФАЙЗЕН БАНК АВАЛЬ» м. Київ,
МФО – 380805, http://www.axxonsoft.com

29.10.2018 № 20181029/01

АКТ
внедрения результатов диссертационной работы
Юбузовой Халичи Ибрагимовны
«Методы безопасного распределения ключей на базе протоколов квантовой криптографии» на соискание ученой степени доктора философии (PhD) по специальности 6D070400 – Вычислительная техника и программное обеспечение

Результаты научных исследований Юбузовой Х.И. внедрены и используются в деятельности ООО "АКССОНСОФТ" с целью обеспечения защищенности и повышения уровня помехоустойчивости разрабатываемых интеллектуальных интегрированных систем безопасности.

В частности, используется предложенная тритовая система помехоустойчивого кодирования и модели, разработанные соискателем для квантово-криптографических систем:

1) модель контроля подслушивания позволяет повысить скорость распределения ключей шифрования при обеспечении защищенности от атак;

2) модель передачи сообщений позволяет повысить уровень доступности квантового канала.

В совокупности, использование приведенных научных разработок позволило повысить уровень доступности каналов связи минимум на 3,8%.

Директор ООО "АКССОНСОФТ" _____ **А.В. Куринной**

Вик. Шинкарюк І.А. т. (044) 220-11-24