ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА
на диссертационную работу Махорина Дмитрия Алексеевича
на тему «Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи»,
представленную на соискание ученой степени кандидата технических наук по специальности
05.11.07 – Оптические и оптико-электронные приборы и комплексы

Актуальность темы диссертации.

Диссертационная работа Д.А. Махорина относится к разработке и исследованию одной из перспективных систем конфиденциальной связи, основанной на использовании принципов квантовой оптики для создания безусловно защищенной системы квантового распределения ключа (КРК) с симметричным шифрованием, функционирующей в режиме «одноразового блокнота».

Для волоконно-оптических линий связи (ВОЛС), являющихся основными каналами скоростной связи, эти исследования особо актуальны, так как ряд вопросов, связанных с адаптацией известных протоколов КРК для ВОЛС, моделей узлов и элементов систем КРК до сих пор изучены недостаточно полно. В связи с этим, выбранная диссертантом тема исследования является актуальной.

Обоснованность и достоверность научных достижений, выводов и рекомендации.

Автором диссертации проведено теоретическое обоснование решений поставленных научных задач, подкрепленное соответствующими расчётными экспериментами. Указанные задачи по моделированию помехоустойчивости волоконно-оптической системы КРК с учетом различных шумовых механизмов в приёмном оптическом модуле, разработке и исследованию подсистем статистического и интерференционного контроля КРК, а также метода временного кодирования, реализующего логику протокола BB84, проведено автором апробированными методами научных исследований, нашедшими научное признание в области квантовых криптографии. Анализ полученных автором расчётных результатов подтверждает обоснованность научных достижений, выводов и рекомендаций диссертационной работы. Обоснованность и достоверность сформулированных автором результатов, подтверждается также их согласованностью с экспериментальными данными, полученными другими исследователями.

Научная новизна результатов диссертации.

Автором предложено решение проблемы адаптации протокола BB84 к волоконно-оптическому квантовому каналу за счёт применения системы кодирования одиночных фотонов в формате time-bin кубитов. Такая система до сих пор не была в центре внимания разработчиков систем КРК. Поэтому описание процессов обработки tb-кубитов при фомировании «сырого» ключа в системе КРК, а также результатов соответствующих расчётных экспериментов является новым.

Новыми являются и способы обнаружения атак на квантовый канал, основанные на использовании данных о состоянии кубитов на выходе квантового канала связи, не прошедших процедуру протокольного согласования базисов, а также результаты обработки динамического распределения сигналов по тайм-слотам в пределах тактового интервала на выходе приёмного оптического модуля (ПрОМ).

Вопросы разработки и оптимизации однофотонных приёмных устройств отражены в ряде публикаций отечественных и зарубежных ученых. Тем не менее, для оценки помехоустойчивости ПрОМ систем КРК автором оригинально использованы известные математические модели, что говорит о научной новизне результатов диссертации.

Значимость результатов для науки и практики.

Рассматриваемая диссертационная работа, по моему мнению, представляет практическую ценность. Рекомендации автора по структуре системы КРК с квантовым каналом на основе ВОЛС потенциально позволяют снизить затраты на техническое оснащение систем КРК, поэтому привлекательны для разработки бюджетных систем защищенной связи.

Оценка содержания диссертации.

Диссертационная работа изложена на 132 страницах, состоит из введения, 4-х глав и выводов.

В первой главе дан обзор современных представлений о принципах построения систем квантового распределения ключа (КРК). Изложен необходимый для создания модели КРК формализм квантовой механики, в том числе описание состояний отдельных квантовых частиц, а также статистические характеристики ансамблей фотонных состояний. Описаны эффекты интерференции амплитуд вероятности этих квантовых частиц, их регистрации и измерения.

Вторая глава диссертации «Функциональные характеристики и схемотехника ПрОМ системы КРК» посвящена описанию аппаратной части системы КРК, а также модели ее функциональных характеристик, описанию проведенных автором расчётных экспериментов.

Вторая половина раздела посвящена обобщению модели трансформации time-bin кубитов в системе последовательно включенных разбалансированных интерферометров Маха-Цендера (ИМЦ).

В третьей главе диссертации «Исследование системы КРК с использованием временных сдвигов одноуровневых состояний одиночных фотонов» автором изложены результаты исследования моделей известных систем КРК, основанных на методе временного кодирования, предложенных С.Н. Молотковым (M04) и Debuisschert T., Boucher W. (DB04) и дополненных подсистемами статистического и интерферометрического контроля в соответствии с темой и задачами представленной работы.

Четвертая глава диссертации «Система КРК-ВК на основе неортогональных tb-кубитов» посвящена разработке и исследованию оптоволоконной системы КРК, работающей по предложенному автором

протоколу BB84 с кодированием квантовых частиц двухуровневыми динамическими состояниями. Здесь автором рассмотрены логический и физический уровни протокола, показана их защищённость как от попыток подмены кубитов, так и от простого копирования и передачи полученных состояний.

Автореферат и публикации автора достаточно полно отражают содержание и основные положения представленной диссертационной работы

Публикации, отражающие основное содержание диссертации

Основные положения диссертации опубликованы автором в 13 печатных работах, из которых восемь статей в журналах, входящих в перечень ведущих рецензируемых научных журналов и изданиях в соответствии с требованиями ВАК Минобразования и науки. В этих трудах полностью отражено содержание диссертации.

К содержанию диссертации имеются следующие замечания:

1. В первой главе автор детально описывает лишь один протокол КРК BB84. При этом в работе отсутствует анализ других существующих протоколов и методов оценки их качества.
2. В работе мало уделено внимания организации и проведению натурных экспериментов по исследованию как всей системы КРК, так и ее подсистем и отдельных блоков.
3. Автором не освещаются важные для полноценной инженерно-технической реализации системы КРК по оптическому волокну с использованием tb–кубитов вопросы, касающиеся процедур обработки «сырого» ключа и коррекции квантовых ошибок. От решения этих вопросов зависят технические и экономические показатели системы.
4. В разделе 2.6 диссертации «Аппаратная платформа системы КРК» не дано обоснование элементной базы аппаратной платформы блоков приёмного и передающего модулей, построенной на основе микросхем ONET4201LD, ONET4211LD, HFBR-25X6Z, ONET4201PA и др.
5. В заключении вместе с итогами исследования была бы весьма уместной оценка перспектив по использованию результатов диссертационной работы с указанием числовых показателей.

Оценка диссертации в целом.

В целом, несмотря на указанные выше замечания диссертационная работа Махорина Д.А. производит положительное впечатление. Она является цельным, завершенным научным исследованием, посвященным актуальной научной проблеме, содержит признаки научной новизны, отвечает принятым критериям достоверности.

Заключение

Считаю, что в диссертационной работе Махорина Дмитрия Алексеевича решены основные поставленные задачи исследования. Основные выводы и рекомендации имеют научную новизну и практическую значимость. Диссертация Махорин Д.А. «Модель системы квантового распределения ключа

с временным кодированием по волоконно-оптической линии связи» является завершенным научным трудом и отвечает требованиям п. 9 «Положения о порядке присуждения ученых степеней» ВАК Минобразования и науки РФ. предъявляемым к кандидатским диссертациям. В ней решены задачи по исследованию и разработке новых методов, которые могут быть положены в основу создания защищенных систем связи нового поколения. Махорин Дмитрий Алексеевич заслуживает присуждения ученой степени кандидата технических наук по специальности 05.11.07 – «Оптические и оптико-электронные приборы и комплексы».

Официальный оппонент
заведующий кафедрой «Информационная безопасность
телекоммуникационных систем»
института компьютерных технологий и информационной безопасности
инженерно-технологической академии
ФГАОУ ВО «Южный федеральный
университет», г. Ростов-на-Дону,
Заслуженный работник высшей школы РФ,
доктор технических наук, профессор

Константин Евгеньевич Румянцев

31 мая 2016 года

Подпись официального оппонента К.Е. Румянцева заверяю.
Директор института компьютерных технологий и информационной безопасности инженерно-технологической академии Южного федерального университета, доктор технических наук, доцент

Геннадий Евгеньевич Веселов

31 мая 2016 года

Служебный адрес: 347928, Россия, г. Таганрог, Ростовская область, ГСП-17А, ул. Чехова, 2, ЮФУ. Тел.: 8-928-182-72-09. E-mail: rke2004@mail.ru