ОТЗЫВ

на автореферат диссертации Махорина Дмитрия Алексеевича «Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи», представленной на соискание ученой степени кандидата технических наук по специальности 05.11.07 – «Оптические и оптико-электронные приборы и комплексы

Защита информационных потоков в телекоммуникационных каналах от нелегитимных пользователей всегда являлась важной задачей для разработчиков аппаратуры защищенной связи. Стремительное развитие арсенала программно-аппаратных средств, с одной стороны, и увеличение объемов передаваемой информации, с другой, явилось вызовом для поиска принципиально новых способов ее защиты. Один из таких способов основан на отображении данных в канале связи в соответствующие криптограммы по методу симметричного шифрования Жильбера Вернама. При этом, как алгоритм генерации необходимого для этой процедуры ключа, так и способ его безопасной доставки легитимным пользователям канала связи основан не на математических процедурах, а на физических законах, описывающих поведение одиночных квантовых частиц (фотонов) в канале связи. В литературе такой способ, теоретически обеспечивающий безусловную защищенность канала, называется квантовым распределением ключа (КРК). Внедрение квантовых алгоритмов, таких как КРК, в массовые технологии требует проведения обширных фундаментальных и прикладных научных исследований. В данной связи, диссертационная работа Махорина Д.А., посвященная исследованию КРК с временным кодированием по волоконно-оптической линии связи, является, несомненно, актуальной.

Полученные Махориным Д.А. научные результаты являются новыми и хорошо отражены в его научных публикациях. Наиболее интересными из этих результатов, на мой взгляд, является предложенный автором способ временного кодирования одиночных фотонов с использованием разбалансированных интерферометров Маха-Цендера для приготовления tb-кубитов, устойчивых при передаче по оптическому волокну на большие расстояния. Судя по автореферату и публикациям, Махориным Д.А. проведены необходимые разработка и исследование компьютерной модели такой системы, определены требования к ее аппаратной и программной частям.

По автореферату можно сделать следующие замечания.

1. На стр.8 автором приведена формула (2) для скорости B формирования системой КРК предварительного ключа $\mathbf{k}_{АБ,}$ учитывающая фактор k_p снижения B для различных протоколов КРК. В работе, однако, отсутствуют сведения о значении

соответствующего коэффициента k_p, как для модифицированного автором протокола С. Молоткова, так и для предлагаемого им протокола, основанного на использовании tb-кубитов.

2. Из рис.5 автореферата видно, что для кодовых состояний базисов протокола С. Молоткова, взятых автором в качестве прототипа, равновероятно появление символов 0 и 1 в любой момент времени тактового интервала. Такая балансировка вероятностей появления указанных символов, очевидно, нарушена в аналогичном авторском варианте состояний базисов tb-кубитов, показанном на рис. 11 автореферата. В данной связи возникает вопрос о возможном снижении защищенности предлагаемого автором протокола.

Указанные замечания не снижают общую положительную оценку диссертации.

Считаю, что рассматриваемая работа является завершенным научным трудом и отвечает требованиям ВАК, предъявляемым к кандидатским диссертациям, а ее автор, Махорин Дмитрий Алексеевич, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.11.07 – «Оптические и оптико-электронные приборы и комплексы».

Доктор физико-математических наук
профессор В.И. Балакший

Подпись доктора физико-математических наук, профессора физического факультета МГУ В.И. Балакшия удостоверяю.