Отзыв

на автореферат диссертации Махорина Д.А. «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»

Работа посвящена актуальной задаче разработки методов квантового распределения ключа в системах секретной связи на основе симметричных шифров. Методы квантового распределения ключа (КРК) обеспечивают безусловную защищенность от перехвата данных и используют различные способы кодирования квантовых состояний. Каждый из способов обладает собственными ограничениями. В работе проведено построение и исследование программной и аппаратной моделей системы КРК с временным кодированием одно- и двухуровневых однофотонных состояний на основе протоколов M04 и BB84.

Для повышения защищенности рассматриваемых систем КРК предложено использование подсистем статистического и интерферометрического контроля состояний квантовых частиц. Рассмотрены варианты их программно-аппаратной реализации. Показана возможность детектирования присутствия в системе нелегитимного пользователя за счет статистики срабатывания приемного оптического модуля, динамического распределения кубитов по тайм слотам в пределах тактового интервала, использования данных о состояниях кубитов, не прошедших протокольную процедуру согласования базисов.

Практическая ценность работы заключается в создании программного комплекса системы КРК, симуляционном и натурном определении параметров предложенной модели КРК, оценке помехоустойчивости приемного оптического модуля и скорости генерации ключа, разработке схемы контроллера на основе формирователя импульсов напряжения с разрядной линией для ЛФД, работающего в гейгеровском режиме и обеспечивающего длительность импульса на выходе формирователя около одной наносекунды.

В качестве замечаний к автореферату следует отметить структурное расположение базовых протоколов модели КРК во второй половине работы, главах 3 и 4, после описания аппаратной части, что несколько затрудняет восприятие предложенных в работе модификаций КРК.

В целом работа Махорина Д.А. соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.11.07 – «Оптические и оптико-электронные приборы и комплексы»

Заведующий кафедрой защиты информации
Новосибирского государственного технического
университета, кандидат технических наук, старший
научный сотрудник В.А. Трушин

Доцент кафедры защиты информации
Новосибирского государственного технического
университета, кандидат физико-математических наук Ю.А. Котов

Подпись В. А. Трушина и Ю.А. Котова заверяю . К. Пустовалова