ОТЗЫВ

на автореферат диссертации Жиляева Андрея Евгеньевича «методика построения сетей квантового распределения ключей смешанной топологии», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

В системах защищенной связи по прежнему актуален вопрос о распределении ключей между пользовательскими устройствами. Судя по автореферату диссертанта Андрея Евгеньевича Жиляева, видно, что соискатель глубоко и всесторонне рассмотрел поставленные задачи в этой области.

Тема диссертации и ее цель - развитие методического обеспечения квантовых коммуникаций для повышения защищенности сетей квантового распределения ключей смешанной топологии. Разработанная структура комплекса защищенной передачи данных, интегрированного с аппаратурой квантового распределения ключей, отличается от известных учетом целостности и конфиденциальности общих секретов в процессе передачи в средства защиты информации (СЗИ) и контролем идентичности сформированных секретов, объединением классического канала аппаратуры квантового распределения ключей (КРК) с транспортным каналом СЗИ для повышения защищенности классического канала аппаратуры КРК.

Предложена методика построения сети КРК смешанной топологии, включающая требования к структуре сети КРК, способу ее функционирования, методику распределения квантовозащищенных ключей, отличающаяся от известных полностью децентрализованным управлением при создании квантовозащищенных ключей, учетом требований их целостности и конфиденциальности, а также имеющая по сравнению с зарубежными аналогами большую гибкость при масштабировании сети. Выносимые на защиту положения следует признать ценными как с точки зрения теоретического значения, так и с точки зрения практического применения.

К автореферату имеются следующие замечания:

1. В предложенной методике построения сети квантового распределения ключей остается этап предварительной доставки ключей доверенным курьером. Из автореферата не очевидно преимущество предлагаемого решения по сравнению с доставкой сразу большого объема ключей на

электронном носителе курьером к местам расположения пользовательских устройств, реализующих процесс шифрования информации.

2. Вопрос синхронизации ключей в автореферате по умолчанию возлагается на номер не квантового исходного ключа, что при последующем производстве квантовых ключей может внести путаницу.

3. В автореферате указано, что для распределения общего секрета необходимо определить цепочку узлов сети КРК, по которой будет производиться распределение. Способ формирования такой цепочки и возможность ее технической реализации не показан в тексте автореферата.

Вышесказанные замечания не снижают общей положительной оценки данной научно-исследовательской работы соискателя в целом.

С учётом вышеизложенного диссертация на тему «Методика построения сетей квантового распределения ключей смешанной топологии» на соискание учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность (технические науки)» соответствует критериям п.9 действующего Положения о присуждении учёных степеней, а её автор Андрей Евгеньевич Жиляев заслуживает присуждения ему степени кандидата технических наук.

Заместитель генерального директора
АО «Конструкторское бюро «Корунд-М»
Доктор физико-математических наук Баранов А.П.

Адрес: Москва, Электролитный пр., 9, корп. 1
Телефон: +7 (499) 678-20-60
Эл. Почта: baranov.ap@yandex.ru

Подпись Баранова Александра Павловича подтверждаю:

Советник Генерального директора Радинский С.С.

Акционерное общество «Конструкторское бюро «Корунд-М» ОГРН 1107746619683 АО КБ «КОРУНД-М» №2 МОСКВА