СПОСОБ ВЫСОКОСКОРОСТНОГО КВАНТОВО-КРИПТОГРАФИЧЕСКОГО ОБМЕНА ИНФОРМАЦИЕЙ С КОНТРОЛЕМ ЕЕ НЕСАНКЦИОНИРОВАННОГО РАСКРЫТИЯ И ЦЕЛОСТНОСТИ

А.М. Тимофеев

При реализации систем криптографической защиты информации одним из наиболее важных этапов является экспорт и импорт критических объектов, в качестве которых могут выступать криптографические ключи, параметры криптографических алгоритмов и пр. Экспорт и импорт таких объектов с использованием телекоммуникационных каналов связи требует защиты объектов для предотвращения их несанкционированного раскрытия и/или модификации, что обеспечивается преимущественно квантово-криптографическими способами, которые, в сравнении с прочими (криптографическими, аппаратными, алгоритмическими и др.), обеспечивают абсолютную защищенность критических объектов [1]. Однако известные квантово-криптографические способы имеют достаточно сложную процедуру согласования базисов, в которых передаются и принимаются символы, что не позволяет выполнять высокоскоростной экспорт и импорт критических объектов по телекоммуникационным каналам связи [1]. В связи с этим целью данной работы являлась разработка высокоскоростного квантово-криптографического способа экспорта и импорта критических объектов по волоконно-оптическим каналам связи. В работе получены выражения для оценки пропускной способности волоконно-оптического канала связи, вероятности ошибки и длительности времени регистрации передаваемых символов. Предложен способ экспорта и импорта критических объектов по волоконно-оптическому каналу связи, позволяющий уменьшить ошибку передачи данных, связанную с деполяризацией оптического излучения, упростить процедуру согласования базисов, в которых переданы и приняты символы, и повысить за счет этого скорость передачи и приема критических объектов.

Литература

1. Квантовая криптография: идеи и практика / С.Я. Килин [и др.]. – Минск, 2007.

ОЦЕНКА ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ: ПРОБЛЕМЫ И РЕШЕНИЯ

В.А. Трушин, А.В. Иванов

При оценке защищенности речевой информации от утечки по техническим каналам в качестве показателя защищённости принято использовать коэффициент словесной разборчивости *W*. Используемая в настоящее время методика определения *W* [1] основана на формантном методе Покровского Н.Б., который был в свое время разработан прежде всего для оценки качества каналов связи [2], что и обусловило ряд некорректностей в существующем методе, а именно:

– проводимые Покровским Н.Б. артикуляционные испытания с использованием некоррелированных таблиц не отражает реалии задач защиты речевой информации, где присутствуют связные, содержательные тексты;

– не учтена возможность записи переговоров с последующим их многократным прослушиванием;

– разбиение частотного диапазона на октавные полосы не отражают специфику слухового аппарата человека, где анализ речевого сигнала осуществляется по критическим полосам;

– в существующей методике (по сути методике косвенных измерений) совершенно не рассматриваются вопросы погрешности *W*, что противоречит ФЗ РФ «Об обеспечении единства измерений».

В докладе приводятся результаты исследований, посвященных решению вышеуказанных проблем.

Литература

1. Железняк, В.К. Некоторые методические подходы к оценке эффективности защиты речевой информации / Ю.К. Макаров, А.А. Хорев // Специальная техника. – 2000. – № 4. – С. 39–45.

2. Покровский, Н.Б. Расчет и измерения разборчивости речи / Н.Б. Покровский. – М.: Связьиздат, 1962. –390 с.