организационных, научных, производственных, технических и экономических мер, направленных на эффективное использование энергетических ресурсов, вовлечение в хозяйственный оборот возобновляемых источников энергии, а также снижение средств, расходуемых на оплату энергоресурсов.

В 2002 году в Ульяновске разработана городская программа «Энергосбережение в г. Ульяновске на период до 2006 года».

Реализация государственной энергосберегающей политики в г. Ульяновске должна обеспечить экономическую заинтересованность энергопроизводителей и потребителей в экономии энергетических ресурсов, сократить финансовые затраты потребителей, включая население, на оплату потребляемых ТЭР.

Целью Программы является достижение реальной экономии энергоресурсов и средств, расходуемых на их оплату.

Основные задачи Программы:

- анализ существующего положения в энергосбережении г. Ульяновска;
- разработка нормативно-правовых актов и финансово-экономических механизмов реализации Программы;
- энергоаудит, проведение энергетических обследований организаций и объектов муниципальной сферы;
- энергоучет, оснащение приборами учета жилищного фонда и организаций бюджетной сферы;
- создание системы сопровождения выполненных мероприятий (сервисная служба);
- энергосбережение в системе тепло-, водо- и энергоснабжения г. Ульяновска;
- разработка оптимальной схемы энергосбережения г. Ульяновска;
- энергосбережение в жилищно-коммунальном секторе;
- повышение квалификации кадров;
- энергосбережение в строительном комплексе;
- энергосбережение на транспорте;
- развитие нетрадиционной и малой энергетики;
- информационное обеспечение энергосберегающей политики в г. Ульяновске.

Реализация Программы энергосбережения проводится в два этапа. На первом этапе (2002-2003 г.г.) должны быть разработаны первоочередные нормативно-правовые и методические документы, необходимые для финансово-экономического механизма обеспечения работ по энергосбережению, и начата реализация первоочередных мер по учету и нормированию энергоресурсов, внедрению энергосберегающих мероприятий.

На втором этапе (2003-2006 г.г.) предлагается совершенствование нормативно-правовой, методической и информационной базы в результате всестороннего анализа выполнения работ первого этапа, продолжить разработку и реализацию проектов и мероприятий по различным направлениям энергосбережения, которые позволят снизить расход энергии и бюджетные затраты на дотацию ТЭР.

Анализ реализации Программы показал, что при отсутствии в городе энергосберегающих мероприятий, только в 2003 году, бюджету города и предприятиям ЖКХ пришлось бы изыскивать на оплату теплоэнергии и ГВС дополнительно 126,6 млн. рублей, в том числе 51,1 млн. рублей по социальной сфере.

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРОТОКОЛА КВАНТОВОЙ КРИПТОГРАФИИ BB84 С КОДИРОВАНИЕМ ОДНОФОТОННЫХ СОСТОЯНИЙ ПО ПОЛЯРИЗАЦИИ

Хайров И.Е., Румянцев К.Е.,
Новиков В.В., Троцюк Е.В.
Таганрогский государственный радиотехнический университет, Таганрог

В настоящее время во всем мире уделяется повышенное внимание к системам передачи конфиденциальной информации. Одним из наиболее перспективных и достаточно новых направлений в области криптографии является квантовая криптография. Как показывают исследования в данной области, сочетание квантово-криптографических методов распределения секретного ключа и классических методов шифрования позволит создать фундаментально защищенные системы передачи конфиденциальной информации.

Одним из наиболее распространенных в настоящее время протоколов квантовой криптографии является протокол BB84. В данном протоколе однофотонные состояния могут быть промодулированы по поляризации или по относительной фазе. Каждый из этих методов модуляции имеет свои преимущества и недостатки. В частности, поляризационная модуляция наиболее предпочтительна при передаче данных по открытому оптическому каналу, в то время как модуляция по относительной фазе может быть использована в волоконно-оптических системах связи.

В работе исследуется эффективность протокола квантовой криптографии BB84 с кодированием однофотонных состояний по поляризации. С этой целью разработан пакет программ для ЭВМ, которые позволяют учитывать как параметры передающего и приемного модулей, так и параметры квантового канала связи. При генерации последовательности фотонов на передающем модуле в модели возможны две ситуации:

1) Количество фотонов за длительность оптического импульса строго фиксировано. Данная ситуация позволяет оценить эффективность протокола при использовании идеального однофотонного или многофотонного лазера.

2) Количество фотонов за длительность оптического импульса случайно и подчинено закону Пуассона с заданным средним $\overline{n}$. При этом генерация псевдослучайного числа n, имеющего распределение Пуассона со средним $\overline{n}$, осуществлялась по методу, предложенному Каном. В процессе моделирования проведен анализ этого алгоритма [1]. Сгенерированная таким образом последовательность случайных величин имеет математическое ожидание и дисперсию, отличающиеся от значения $\overline{n}$ на сотые доли

процента. Это подтверждает правомерность использования предлагаемого алгоритма генерации случайных чисел по закону Пуассона.

В качестве параметра фотоприемного модуля использовалась его квантовая эффективность, характеризующая вероятность преобразования оптического сигнала в электрический. Данный параметр, наряду с шумовыми свойствами фотоприемной аппаратуры, является одним из определяющих эффективность всей системы связи.

При моделировании квантового канала связи учитывались потери оптического излучения связанные с поглощением и рассеянием излучения. Так же, моделировалась ситуация наличия в канале перехватывающего агента. При этом исследовались две ситуации:

1) Перехват и генерация злоумышленником всех фотонов за длительность оптического импульса. Данная ситуация позволяет моделировать реальные системы связи.

2) Отбор только одного фотона за длительность импульса. Эта ситуация позволяет оценивать эффективность протокола квантовой криптографии при наличии злоумышленника с идеальной аппаратурой, позволяющей осуществлять несанкционированный съем.

Таким образом, проведенные исследования позволили оценить эффективность протокола квантовой криптографии BB84 при использовании поляризационной модуляции.

Список литературы

1. Радиоэлектронные технологии информационной безопасности: Сборник научных статей / Под. ред. К.Е. Румянцева. – Таганрог: ТРТУ, 2002. – С. 145-155.

АНАЛИЗ МЕТОДОВ ФОРМИРОВАНИЯ КЛЮЧЕВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ В МНОГОПОЛЬЗОВАТЕЛЬСКИХ КВАНТОВЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Хайров И.Е., Румянцев К.Е.,
Новиков В.В., Троцюк Е.В.
Таганрогский государственный радиотехнический университет, Таганрог

Бурное развитие в последние годы квантовых компьютеров и связанных с ними технологий привело к появлению ряда революционных достижений, способных значительно ускорить научно-технический прогресс. К таким достижениям относится квантовая криптография.

Генерация ключа методами квантовой криптографии осуществляется непосредственно в процессе передачи единичных фотонов по каналу связи. Надежность этих методов базируется на незыблемости фундаментальных законов квантовой физики.

Квантово-криптографические системы первоначально использовались для связи отдельных пар пользователей. Однако актуальным является разработка и исследование подобных методов для связи большого количества пользователей. Работа в данном направлении активно ведется как зарубежными, так и отечественными научными центрами.

Как показали исследования известные методы распределения секретного ключа используют либо древовидную топологию сети, либо кольцевую с необходимостью использования дополнительных каналов обмена информацией. В частности методы квантовой криптографии могут использоваться при построении пассивной оптической сети, содержащей центральный сетевой контроллер, связанный посредством пассивного оптического светоделителя с множеством сетевых пользователей. В этой схеме используется квантовое поведение оптического светоделителя. Соответственно каждый пользователь будет обеспечен уникальным произвольно выбранным подмножеством битов.

Другая квантово-криптографическая система содержит квантовый канал связи с множеством узлов, включающих передающий и приемный модули, связанные с квантовым каналом связи. Передающий модуль генерирует световой сигнал, представляющий собой последовательность фотонов, для распределения через квантовый канал. Получатель сообщения принимает световой сигнал, посланный передатчиком и измеряет квантовые состояния этого сигнала. Данный метод организации оптической сети использует кольцевую топологию, однако основным ее достоинством является то, что каждый из пользователей может быть инициатором обмена данными.

В связи с этим, актуальной является проблема разработки метода распределения секретного ключа между большим количеством последовательно расположенных пользователей без дополнительных каналов обмена информацией. В работе предложен новый метод организации оптической сети, в которой происходит распределение секретного ключа с использованием квантовой криптографии. Данный метод основан на принципе измерение–повторная отправка и применим в системах с модуляцией по поляризации.

Исследования так же показали, что при непосредственном использовании данного метода, процесс обмена характеризуется большим процентом ошибок. Однако, с введением в рассматриваемую сеть подсистемы синхронизации между поляризационными анализаторами пользователей, данный метод будет соответствовать протоколам, применяющимся для обмена данными между несколькими пользователями.

Данная оптическая сеть распределения секретного ключа методами квантовой криптографии может быть также отнесена к сети связи с кольцевой топологией.

Основной проблемой практической реализации подобной оптической сети, является обеспечение точной синхронизации поворотов поляризационных анализаторов большого количества последовательно расположенных пользователей. Так как вероятность прохождения поляризованного фотона через анализатор пропорциональна косинусу угла между направлением поляризации и осью анализатора, то неточность синхронизации может составлять единицы градусов.