И.Е. ХАЙРОВ (к.т.н., доцент), **К.Е. РУМЯНЦЕВ** (д.т.н., профессор), **Д.И. СЕРОГОДСКИЙ** (студент), **С.В. НОСКОВ** (студент), **М.Г. КОТЕГОВ** (студент)
(Таганрогский государственный радиотехнический университет)

АНАЛИЗ КВАНТОВО-КРОПТОГРАФИЧЕСКОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ С ПОЛЯРИЗАЦИОННЫМ КОДИРОВАНИЕМ ОДНОФОТОННЫХ ИМПУЛЬСОВ

Проблема защиты информации от несанкционированного доступа является актуальной в связи с широким распространением компьютерных и телекоммуникационных систем. Изучением методов шифровки занимается криптография. В последнее время в этой области идёт активная работа над принципиально новым методом защищенного распределения ключевой информации – квантовой криптографии.

Задача квантовой криптографии заключается в передаче случайных последовательностей бит, которая затем может быть использована в качестве ключа для кодирования и декодирования сообщений.

Квантовая криптография опирается на фундаментальную неопределенность поведения квантовой системы – невозможно одновременно достоверно измерить координаты и импульс частицы, а так же два не ортогональных состояния поляризации фотона. Это фундаментальное свойство природы в физике известно как принцип неопределенности Гейзенберга.

В квантовой криптографии разработано несколько протоколов. Наиболее распространённым и используемым в практических приложениях является протокол BB84. В данном протоколе для кодирования однофотонных импульсов используется модуляция оптического излучения по поляризации или по относительной фазе. Системы с фазовым кодированием наиболее предпочтительны в ВОЛС, а система с поляризационным кодированием наиболее распространены в открытых системах связи (атмосферных, космических) и в ВОЛС с использованием волокон специальных конструкций. К ним относятся волокна с сохранением поляризации, например, с сердцевиной в виде спирали.

В данной работе рассматривается протокол BB84 с кодированием по поляризации. Особенность данного протокола является то, что на передаче используется четыре неортогональных состояния поляризации (0°, 45°, 90° или 135°).

Идея квантовой криптографии с поляризационным кодированием заключается в следующем. Поток горизонтально поляризованных фотонов полностью проходит через горизонтальный анализатор. Если поворачивать анализатор вокруг своей оси, то поток пропускаемых фотонов будет уменьшаться до тех пор, пока при повороте на 90° ни один фотон не сможет пройти анализатор. При повороте фильтра на 45° он пропустит горизонтально поляризованный фотон с вероятностью 50%.

Таким образом, измерить поляризацию света можно лишь тогда, когда заранее известно, в каком базисе он был поляризован. Если известно, что свет поляризован либо вертикально, либо горизонтально, то пропустив его через горизонтальный фильтр, мы узнаем по результату, была ли поляризация 0 или 90°. Если поляризация была диагональной, а анализатор установлен горизонтально, то по результату невозможно сказать, был ли свет поляризован на 45° или 135°.

В связи с этим, при непосредственном вмешательстве в сеанс "квантовой связи" возникает большое количество ошибок, что достоверно выявляется легальными пользователями.

Основной принцип генерации квантового ключа на основе протокола BB84 [1] заключается в том, что передающая сторона подготавливает однофотонные состояния с линейной поляризацией в двух не ортогональных друг другу базисах. Один – назовем его вертикально-горизонтальным – с поляризацией фотонов 0° и 90°. Второй – назовем его диагональным – с поляризацией 45° и 135°. Передающая и приемная стороны договариваются о коде каждой поляризации в двоичном представлении, например, фотоны с поляризацией 0° и 45° обозначают цифру "0", а фотоны с поляризацией 90° и 135°

обозначают цифру "1". Во время передачи осуществляется посылка последовательности фотонов, поляризация которых выбрана случайным образом, и может составлять 0°, 45°, 90° и 135°. Приемник регистрирует пришедшие фотоны, и для каждого из них случайным образом выбирает базис измерения. Далее после осуществления нескольких процедур усиления секретности формируется секретный ключ известный только двум пользователям. Таким образом, зашифрованную этим ключом информацию смогут расшифровать только легальные пользователи.

В заключении необходимо отметить то, что данные системы реализованы в практических приложениях. В начале июня 2004 года в Кембридже (штат Массачусетс, США) была запущена в эксплуатацию первая в мире компьютерная сеть с квантовой криптографией. Система Quantum Net (Qnet) в настоящее время состоит из шести серверов, которые способны взаимодействовать с обычными узлами Всемирной паутины и пользователями Интернета.

Предполагается, что квантовые криптосистемы заинтересуют военные организации и коммерческие компании, регулярно сталкивающиеся с необходимостью передачи секретных данных. Правда, у подобной системы защиты есть существенный недостаток: протяженность линий связи пока не может превышать 120 км из-за "деградации" фотонного сигнала.

Таким образом, в результате проведенной работы выявлены основные направления развития квантово-криптографических систем передачи конфиденциальной информации.

1. Bennett Ch.H., Bessette F., Brassard G., Salvail L., Smolin J. //J. Cryptology. 1992. V. 5. P. 3.