дет корректно принят получателем, так как этот процесс носит вероятностный характер. Во-вторых, существенной особенностью системы является использование однофотонных оптических импульсов, что сильно снижает скорость передачи по каналу связи. В силу указанных причин квантовый канал связи малопригоден для передачи больших объемов данных, а больше подходит для выработки секретного ключа, который будет использован легальными пользователями для шифрования данных [1, 2].

В идеальных системах квантовой коммуникации непосредственный перехват данных невозможен, так как он достоверно обнаруживается легальными участниками обмена по возникающим ошибкам в передаче. Однако реальные квантово-криптографические системы отличаются от идеальных. Во-первых, аппаратура участников информационного обмена несовершенна, что приводит к появлению ошибок в приемном модуле даже при отсутствии несанкционированного доступа (НСД). В этих обстоятельствах наличие определенного уровня ошибок не должно восприниматься системой как попытка подслушивания. В то же время, наличие собственного фона ошибок позволяет противнику осуществлять перехват, маскируя неизбежно возникающие при этом искажения под собственные ошибки системы. Во-вторых, в реальных линиях передачи существует затухание сигнала, что вынуждает отправителя увеличивать мощность импульса, т.е. число фотонов в нем. Если импульс содержит много фотонов, поляризованных одинаковым образом, то с помощью светоделителя от него можно сделать отвод и тестировать, не искажая основной сигнал. Понятно, что такой перехват следует осуществлять как можно ближе к отправителю — там уровень сигнала выше. Так же затухание сигнала приводит к увеличению общего уровня ошибок, и у злоумышленника увеличиваются шансы замаскировать перехват под собственные ошибки системы. В-третьих, у злоумышленника есть лучшая стратегия перехвата, чем простое угадывание базиса. Дело в том, что законы квантовой механики запрещают лишь идеальное клонирование квантовой системы. При этом возможно получить копию кванта на основе вынужденного излучения. Имея в распоряжении несколько копий кванта злоумышленник может анализировать их поляризацию в двух различных базисах. Конечно, при этом будут возникать ошибки, но их уровень будет ниже, чем при простом угадывании базиса. И если уровень ошибок при перехвате окажется сопоставим с собственным фоном ошибок системы, прослушивание становится возможным. Поэтому в распоряжении злоумышленника всегда есть возможность перехватить какую-то часть передаваемых битов, замаскировав неизбежно сопровождающие такой перехват ошибки под собственные ошибки системы.

Для отсеивания собственных ошибок в реальных системах квантовой криптографии необходимо применять различные протоколы коррекции, а для снижения значимости перехваченных противником битов нужно использовать процедуру усиления секретности. Для этого проще всего вырабатывать несколько блоков ключа, а итоговый рабочий ключ получать побитовым суммированием по модулю 2 этих блоков. Тогда, чтобы наверняка определить хотя бы один бит ключа, злоумышленнику нужно знать соответствующие биты во всех блоках. Другой возможный метод заключается в том, чтобы вырабатывать ключи из сформированного битового вектора с помощью хэш-функций.

Таким образом, в отличие от идеальных, реальные системы квантовой коммуникации не способны обеспечить абсолютную секретность передаваемых данных. Это обусловлено наличием у них фона собственных ошибок, под которые можно замаскировать попытки перехвата, а также затуханием в каналах связи из-за необходимости использования многофотонных импульсов. Последнее делает возможным неразрушающий перехват данных и является практически неустранимым фактором.

СПИСОК ЛИТЕРАТУРЫ

1. Румянцев К.Е., Хайров И.Е., Новиков В.В., Троцюк Е.В. Анализ методов съема информации в квантовом канале связи //Научно-практический журнал "Информационное противодействие угрозам терроризма", - 2004г. №3. С.71-73.

2. Румянцев К.Е., Хайров И.Е., Новиков В.В. Распределения секретного ключа в оптических сетях с кольцевой топологией методами квантовой криптографии //Известия ТРТУ. Специальный выпуск «Материалы 50-й научной конференции». Таганрог: Издательство ТРТУ, 2004.

АНАЛИЗ МЕТОДОВ ПЕРЕХВАТА И ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННОМУ СЪЕМУ ИНФОРМАЦИИ В СИСТЕМАХ КВАНТОВОЙ КРИПТОГРАФИИ С КОДИРОВАНИЕМ ПО ФАЗЕ

Хайров И.Е., Жуков М.А., Полывяная В.В.
Таганрогский государственный радиотехнический университет, Таганрог

Системы квантовой криптографии позволяют обеспечивать защищенное распределение секретного ключа. Однако, несмотря на все преимущества этих систем, все же и к ним возможно осуществить неконтролируемый несанкционированный доступ. Так, например, для систем кодирования Plug-and-Play на практике нет возможности использовать однофотонные импульсы, что дает широкие возможности для перехвата злоумышленнику.

Проанализируем схемы, использующие фазовые модуляторы для формирования квантовых состояний. Здесь обмен информацией осуществляется в две стадии. Сначала по квантовому каналу, затем по обычному каналу, открытому для подслушивания (например, через Интернет).

На первой стадии Алиса выбирает случайно и с равной вероятностью одно из четырех квантовых состояний $|0_A>$, $|0_B>$, $|1_A>$, $|1_B>$, и пересылает его Бобу по квантовому каналу, фиксируя в своих записях значение бита данных и базис, в котором он закодирован.

Боб производит измерение переданного состояния, в одном из двух возможных базисов A или B, выбранном независимо от Алисы. Если базис, выбранный Бобом для измерения, совпадает с базисом, выбранным Алисой для передачи, биты данных у Алисы и Боба будут идентичны. В противном случае они совпадут с вероятностью 50%. Алиса и Боб повторяют эту процедуру N раз, в результате чего каждый из них будет обладать строкой бит длиной N.

На второй стадии общение Алисы и Боба происходит по открытому каналу, который, однако, должен соответствовать следующему условию: Ева не может изменять передаваемые сообщения. Алиса и Боб сообщают друг другу использованные ими при передаче значения базисов и договариваются исключать из своих данных те биты, для которых базисы передачи и детектирования не совпадали. Результирующая строка бит называется сырым ключом.

Ева в свою очередь может перехватывать носители информации, посланные Алисой, измерять их состояния и пересылать далее Бобу. Эта стратегия называется “перехват/регенерация”. Поскольку Ева вынуждена выбирать базисы для детектирования случайно и независимо от Боба и Алисы, то приблизительно в 50% случаев базисы Евы и Боба не совпадут. А так как измерения Боба случайны и примерно на 50% совпадают с данными Алисы, то вероятность правильного результата будет 75%. Это означает, что Алиса и Боб должны сравнить публично некоторое случайно выбранное подмножество своих данных на наличие ошибок.

Существует, однако, еще один способ подслушивания, известный как «расщепление луча». Особенность его состоит в том, что Алиса и Боб не могут определить наличие такого рода подслушивания в канале. Известно, что при используемом повсеместно способе получения одиночных фотонов, а именно, ослаблении лазерного излучения до средней интенсивности I≤1 фотона на импульс, определенная доля выходного излучения будет содержать более одного фотона в импульсе. Таким образом, поставив на пути фотонов обыкновенный делитель, Ева может получить некоторую информацию о ключе, не внося ошибок в передачу.

Все это справедливо лишь для идеального квантового канала, в реальном же канале всегда присутствуют шумы, и некоторое несоответствие в данных Алисы и Боба будет всегда, даже в отсутствие подслушивания. Так как Алиса и Боб не могут различить ошибки, имеющие причиной подслушивание, и ошибки, вызванные естественными шумами канала, то им приходится предполагать, что все ошибки передачи вызваны присутствием Евы. При этом стадия обмена по открытому каналу усложняется.

Рассмотренные атаки объединяет то, что для осуществления подслушивания измерительная аппаратура Евы каким-либо образом взаимодействует с передаваемыми квантовыми состояниями. Однако существует возможность подслушивать эти схемы либо, не имея дела с квантовыми состояниями вообще, либо, детектируя их однозначно при помощи некоторой дополнительной информации, почерпнутой во время передачи. Такой тип атак получил название “троянский конь”. При этом одиночный сканирующий импульс, посланный Евой, вызовет множество отраженных сигналов с различными амплитудами, задержками и фазами, и все они в разной степени пригодны для успешного выполнения данной атаки.

Существуют различные методы защиты данных, передаваемых Алисой. Один из них заключается в постановке аттенюатора на выходе передающего интерферометра. При этом источник одиночных фотонов для передатчика делается путем ослабления лазерных импульсов до средней интенсивности порядка 0,1 фотона на импульс. Для Евы присутствие аттенюатора на выходе приемника будет означать значительное увеличение требуемой мощности лазера.

Еще одним методом защиты является измерение входящей оптической мощности в передающем и приемном интерферометрах для предупреждения легальных пользователей о несанкционированном проникновении в канал. Т.к. для Евы имеется достаточно широкий выбор длин волн, на которых может осуществляться сканирование, то целесообразно использовать узкополосные чувствительные детекторы вместе с полосовыми фильтрами на выходе передатчика и входе приемника, вместо широкополосных измерителей оптической мощности.

РАЗРАБОТКА ПРОГРАММНО-РЕАЛИЗУЕМОГО УЗЛА ДОСТУПА ПАКЕТНОЙ СЕТИ

Юрасов С.В.
Нижегородский Государственный Технический Университет, Н.Новгород

Безусловно, пропускная способность сетей в современном информационном мире невероятно важна. Однако, на сегодняшний день возможности сетевых магистралей таковы, что оптические технологии и современные методы мультиплексирования обещают не только удовлетворить самые высокие требования, но и создать некоторую избыточность полосы пропускания. Тем не менее, ряд приложений, таких, как видео, мультимедиа, передача голоса по IP-сетям, требует не просто «толстых» каналов, а и соответствующего качества обслуживания – QoS (Quality of Service). Иными словами, в сложившейся ситуации на первый план выходит скорость обработки пакетов. И здесь вся нагрузка ложится на активные элементы сетевой инфраструктуры – маршрутизаторы, коммутаторы, *узлы доступа* и другие устройства, участвующие в формировании трафика в пакетных сетях.

Ни для кого не секрет, что для конечного пользователя сеть – это не компьютеры, кабели и концентраторы, и даже не информационные потоки, для него сеть – это, прежде всего, тот набор сетевых служб и услуг, с помощью которых он получает возможность просмотреть список имеющихся в сети компьютеров, прочитать удаленный файл, распечатать документ на «чужом» принтере или послать почтовое сообщение. Именно совокупность предоставляемых возможностей – насколько широк их выбор, насколько они удобны, надежны и безопасны – определяет для