больше, чем первые, подходят под категорию «врач общей практики», однако работать им они не желают и если все же их направить на эту должность, то путного ничего из этого не выйдет, то есть лишив человека мечты государство только теряет будущего талантливого специалиста и не приобретет ничего в замен.

ФЕНОМЕН КОМПЕТЕНЦИЙ

Шараева М.А.
Оренбургский государственный университет, Оренбург

«Независимо от того, являетесь ли Вы преподавателем (шведского) университета или библиотекарем, Вы или утомлены умными словами об информационной грамотности, или никогда об этом не слышали», - считает Nina Ström, координатор программы NordInfoLit, отмечая, что первоначально преподаватели были скептически настроены к информационной компетентности, считая ее, во- первых, прерогативой библиотекарей, во- вторых, что библиотекари универсально квалифицированы для ее передачи. Но, как отмечает российский автор В.Трайнев, «информационное невежество в наши дни ведет к технологическому банкротству и национальному унижению, к превращению страны в сырьевую колонию или свалку устаревшей технологии».

В англоязычных странах понятие «competence» часто отождествляется с «information literacy». Финский автор Savolainen (2002) приравнивает его к навыкам: «competency»=«skill»=«information literacy», считая, что «информационная грамотность - это вектор компетенции». Само слово literacy, согласно Chamber English Dictionary, происходит от латинского litteratus, вытекающего из litera, подразумевающего letter, следовательно, «грамотная персона - та, что владеет письмом», или «learning able to read and write, having a competence in (or with)».

В современной европейской традиции применяется понятие Information Related Competence (IRC) и существует несколько его трактовок.

Первая группа авторов концентрирует свое внимание на изучении проблем высшего образования, особенно на on-line обучении: «IRC - это блок (либо несколько блоков) компетенций, связанных с использованием информационного поиска, процессами отбора, идентификации, локализации информации, атакже ее записью и хранением -информационные процессы, которые варьируются «посредниками», или медиа - источниками».

Вторая группа авторов, рассматривающие обучение как активный, конструктивный, целенаправленный процесс, к которому присоединяется ментальная активность, «конструирование смысла» (sensemaking Бренды Дервин), знания, мнения. IRC здесь представляются как независимые в смысле взаимосвязей и содержимого компетенции, которые интегрируются как «элементы» в конструкцию образовательной среды и соотносятся с характером обучаемого. Это предшествующая сумма знаний, мета- когниции, мотивация.

Третья, немногочисленная, группа ученых придерживается теории «зонтика» (umbrella): IRC -это зонтик, под которым скрываются комбинации комплексных когнитивных умений, от элементарных до высшего порядка.

Keen (1992): «Комбинация составных умений, типа «problem solving» и компетенции типа саморегулирования и «learning-to -learn». Kirscher (1999): «компетенции предполагают способность к гибкому соотношению компетентного поведения».

Итак, в современной науке, занимающейся вопросом компетенций, существуют две основных философии:

-подход к информационной компетенции ориентирован на навык (skill);

-феноменографический подход, зависит от ситуации: кто ищет информацию и по какой причине?

Финский исследователь Anttiroiko назвал это явление «феноменом компетенций».

СПИСОК ЛИТЕРАТУРЫ

Sirje Vircus. Information literacy in Europe: a literature review: Abstract. Information Research, Vol. 8, 4, July 2003. http:www.informationr.net/lr/lraindex.html.

Информационные технологии будущего

АНАЛИЗ ВОЗМОЖНОСТЕЙ ДОСТУПА К КВАНТОВЫМ КАНАЛАМ СВЯЗИ

Хайров И.Е., Дзейкало А.А.,
Носков С.В., Серогодский Д.И., Котегов М.Г.
Таганрогский государственный радиотехнический университет, Таганрог

В настоящее время во всем мире ведутся широкомасштабные исследования в области квантовой криптографии, которая обеспечивает высокую надежность и защищенность передаваемой информации по каналам связи. Если злоумышленник попытается перехватить информацию, передаваемую через квантовый канал, то он внесет в нее большое количество ошибок. Это связано с тем, что фотон, несущий информацию, при детектировании разрушается. После этого злоумышленник генерирует новый квант с параметрами, например поляризацией, соответствующими результату его измерения. В ряде случаев поляризация нового кванта не будет совпадать с той, которая использовалась отправителем, что приведет к искажению данных. Наличие искажений будет обнаружено в ходе сверки легальными пользователями некоторого общего отрезка данных.

Системы квантовой криптографии обладают рядом принципиальных особенностей. Во-первых, нельзя заранее сказать, какой из передаваемых битов бу-

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.