Таким образом, в результате проведённой работы были проанализированы основные способы кодирования однофотонных импульсов, применяемые в квантово- криптографических системах, рассмотрены их достоинства и недостатки. Выявлено, что для передачи информации по волоконно-оптическим линиям связи наиболее предпочтительным является кодирование по относительной фазе.

СПИСОК ЛИТЕРАТУРЫ

1. Charles H. Bennett et al. Experimental Quantum Cryptography, Journal of Cryptology, no. 5, 1992.

2. Wolfgang Tittel, Gregoire Ribordy and Nicolas Gisin. Quantum Cryptography, Physics World, March 1998.

3. Martinelli M., A universal compensator for polarization changes induced by birefringence on a retracting beam. Opt. Commun., 1989, vol. 72, pp. 341-344.

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

Хайров И.Е., Румянцев К.Е.,
Серогодский Д.И., Носков С.В., Котегов М.Г.
Таганрогский государственный радиотехнический университет

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.

СПИСОК ЛИТЕРАТУРЫ

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

Педагогические науки

ОРГАНИЗАЦИЯ СИСТЕМЫ ПСИХОЛОГО-ПЕДАГОГИЧЕСКОГО СОПРОВОЖДЕНИЯ ПРОФИЛЬНОЙ ПОДГОТОВКИ В ШКОЛЕ

Абакумова Н.Н.
Томский государственный университет, Томск

Процессы модернизации образования предъявляют свои требования к осознанному выбору профессиональной карьеры. Современные тенденции рынка труда указывают на появление новых профессий и, вместе с тем, фиксируется изменение социально-психологической атмосферы.

Практический аспект профильного обучения реализуется за счет координации средней школы, профессиональных учебных заведений всех типов, предприятий, средств массовой информации. Помочь школьнику выбрать сферу предметной деятельности, а в ней и профессию, отвечающую его способностям и возможностям, содействовать развитию профессиональных склонностей и интересов – это постоянная практическая работа является основой профессиональной консультации школьного психолога.

Опыт МОУ СОШ № 25, г. Томска и МУ ОСШ № 196, г. Северска по проведению индивидуальных профконсультаций с учащимися 9-11 классов, анкетирования школьников по выявлению уровня: профессионального самоопределения; их информированности о мире профессий; самопознания показали, что необходима целенаправленная работа по информированию о современном рынке труда, проблемах занятости и ряда других вопросов и тем. Цель организации психолого-педагогического сопровождения: способствование личностному и профессиональному самоопределению личности учащегося на разных ступенях обучения.

Профессиональное самоопределение выпускников школ происходит не только на основании рациональных, но и нерациональных мотивов. Учащийся руководствуется не только собственными знаниями, но и советами родителей и друзей, семейными традициями, своей склонностью к каким-либо предметам школьной программы.

Задачи профильного обучения можно ставить, начиная уже с младшего школьного возраста. Однако следует отметить, что ранняя профилизация имеет свои особенности, так как сложно выделить специфические склонности, способности ребенка. Это предопределяет необходимость: а) отказаться от жестокости и категоричности при определении диапазона перспективных для ребенка видов профессиональной деятельности; б) акцентировать внимание на решении задач по развитию способностью ребенка овладевать универсальными, необходимыми практически для всех видов деятельности знаниями, умениями и навыками; в) максимально использовать игровые, эмоционально насыщенные формы коррекционных мероприятий.

Таблица 1.Этапы и формы профессионального самоопределения учащихся

№	Наименование этапа	Возраст	Цели и задачи	Формы и содержание деятельности
1	Эмоционально-образный	Дети старшего дошкольного возраста	Формирование положительного отношения к профессиональному миру (людям труда, их занятиям)	Вырабатывание первоначальных трудовых умений в доступных для ребенка видах детальности
2	пропедевтический	1-4 классы	Формирование добросовестного отношения к труду, помочь в осознании его роли в жизни человека и общества, развитие интереса к профессии родителей и ближайшего производственного окружения, обучение детей пользованию всеми каналами восприятия окружающего мира	Тренинги, игровые занятия, семинары. Например, «Специфические трудности в обучении в младшей школы», «Развитие каналов восприятие окружающего мира у младших школьников», «Общие требования профессии к человеку», «Здоровье и выбор профессии»