Түлкібай Д.Ә.

Шүлембаев Д.Б.

Криптографическая защита информации с помощью квантовой криптографии

В современном мире один из надёжных способов сохранить в тайне все виды переговоры или передаваемые по компьютерным сетям связи информации – это использование квантовой криптографии. Идея применить квантовую криптографию для целей защиты информации используя природу объектов микромира - квантового света (фотонов), поведение которых подчиняется только законам физики, и это применение стала наиболее актуальной и надежной. Несмотря на то, что сегодня уже имеются коммерчески доступные устройства квантовой криптографии, научная компонента в этой области до сих пор прогрессирует.

Наибольшее практическое применение квантовой криптографии найдено сегодня в области защиты информации, передаваемой по волоконно-оптическим линиям связи (далее ВОЛС). Это связано с тем, что оптические волокна позволяют передавать фотоны на большие расстояния с минимальными искажениями. Очевидно, что существующие технологии и стандарты, еще недавно считавшиеся стойкими, становятся постепенно уязвимы, и будут заменены в ближайшее время. Это связано с новыми возможностями расшифровки данных за счет увеличения производительности классических компьютеров, а также с развитием квантовых компьютеров. Таким образом, целью проекта, на первом этапе, является разработка технологий построения высокоэффективных квантовых сетей связи, обеспечивающих наивысшие существующие средства защиты каналов передачи данных от несанкционированного доступа.

Идея использования квантовой криптографии чтобы надежно защитить свои данные принадлежит Стивену Визнеру. Впервые его идея об использование квантовых объектов была предложена в 1970 году. Тогда он, еще являясь студентом

Колумбийского университета, подал статью по теории кодирования в журнал IEEE Information Theory, но она не была опубликована, так как изложенные в ней предположения казались фантастическими, а не научными. В своей статье он описал идею возможности использования квантовых состояний для защиты денежных банкнот. Визнер предложил в каждую банкноту вмонтировать 20 так называемых световых ловушек, и помещать в каждую из них по одному фотону, поляризованному в строго определенном состоянии. Каждая банкнота маркировалась специальным серийным номером, который заключал информацию о положении поляризационного фотонного фильтра. В результате этого при применении отличного от заданного фильтра комбинация поляризованных фотонов стиралась. Но на тот момент технологическое развитие не позволяло даже рассуждать о таких возможностях. Далее на основе принципов и теории Стивена Визнера, были разработаны способы кодирования и передачи сообщений, двумя учёными Чарльз Беннет (Charles Bennett) из фирмы IBM и Жиль Брассард (Gilles Brassard) из Монреальского университета. Ими был разработан доклад на тему «Квантовая криптография». Впоследствии их разработанный протокол признан первым и базовым протоколом квантовой криптографии и был назван в честь его создателей BB84.

На протяжении многих лет, квантовая криптография прошла путь от теоретических исследований и доказательства основных теорий до коммерческих систем, использующих оптическое волокно для передачи информации на расстоянии десятков километров. Экспериментальной демонстрация впервые осуществилась в 1989 году, с установкой квантового распределения ключей, передача осуществлялась через открытое пространство на расстояние 30 сантиметров. Далее эти эксперименты были проведены с использованием оптического волокна в качестве среды распространения. Дальность передачи информации достигала от минимального до максимального расстояния. В связи с этим рекорд по дальности передачи информации принадлежит

объединению ученых Лос-Аламоса и Национального института стандартов и технологий, и он составляет 184 км. В нем использовались однофотонные приемники, охлаждаемые до температур близких к нулевым по Кельвину.

Ссылаясь на все эти эксперименты, можно увидеть, как квантовая криптография была очень популярна для исследования. На ее исследования были потрачены достаточно ресурсов, в том числе можно сказать и годы трудов для ее изучения. Так как квантовая криптография является очень надежным способом для передачи конфиденциальной информации.

Важным на данный момент является то, что большая часть описанного материала в статье уже стало реальностью, перекочевав из теорий в практику, и потихоньку внедряется в технологическую сферу человечества, создавая тем самым большой спрос на развитие квантовой криптографий. Квантовая аппаратура позволяет распределять ключи через квантовый канал на расстояние, превышающее 100 км (рекорд 184 км), со скоростями достаточными для передачи ключей шифрования. Над этим проектом диапазон разработчиков новых технологий квантовой криптографии охватывает не только крупнейшие мировые институты, но и маленькие компании, только начинающие свою деятельность. И все они уже способны вывести свои проекты из лаборатории на рынок. Все это позволяет сказать, что рынок находится на начальной стадии формирования, когда в нём могут быть на равных представлены и те, и другие. На сегодняшний день в мире основными потребителями систем квантовой криптографии в первую очередь выступают министерства обороны, иностранных дел, а также крупные коммерческие объединения. С появлением квантовых компьютеров традиционное шифрование перестанет быть эффективным.

В век информационных технологий информация важна как никогда раньше, и чтобы надежно ее сохранить необходимо идти в ногу со временем и обновлять ее защиту. На сегодняшний день квантовая криптография — это именно то, что необходимо для

надежной и эффективной защиты информации в разных сферах деятельности нашей страны, в том числе и в министерстве обороны

На данный момент использование квантовой криптографии требует большой ответственности. Когда будут созданы подобные криптографические системы, в нашей стране то возникнет другой этнический вопрос. Это значит, что пострадает вся ценная информация, которая передается в зашифрованном виде, под угрозой окажутся банковские транзакции и криптовалюта, злоумышленники смогут получать доступ к критически важным объектам из любой точки мира. Данная проблема затронет не только разведсообщество и экспертов в сфере кибербезопасности, но и социальные платформы и мессенджеры, такие как WhatsApp и другие социальные сети, использующие ключи для авторизации пользователей. А с другой стороны, если данная технология будет доступна только правительству, военным, и спецслужбам. То любая информация, зашифрованная с помощью такой системы, станет неуязвимой к перехвату, даже со стороны спецслужб.

Список литературы

1. К.Е. Румянцев, И.Е. Хайров, “Эффективность волоконно-оптической системы передачи информации”
2. *Килин С. Я., Хорошко Д. Б., Низовцев А. П.* «Квантовая криптография: идеи и практика»
3. Сайт Википедия — свободной энциклопедии https://ru.wikipedia.org/wiki/
4. Сайт свободной энциклопедии http://www.ict.edu.ru