ЭТАПЫ РАЗВИТИЯ КВАНТОВОЙ КРИПТОГРАФИИ

В.К. Кожеваткин, В.А. Бердников

Поволжский государственный университет сервиса, Тольятти, Россия

Обоснование. Квантовая криптография используется в различных областях, в том числе в банковском секторе, государственных структурах, военной отрасли и частном торговом секторе. Начальный этап, при котором началось строительство всей квантовой системы, произошло в 1970 г. и продолжается по сей день, что подтверждает факт востребованности способа защиты данных. Стоит отметить, что важное требование, при развитии в дальнейшем этой отрасли — это секретность и безопасность при передаче данных. Сама квантовая криптография представляет способы защиты информации, разработанные на определенных явлениях. Для обеспечения защиты информации в квантовой криптографии рассматриваются случаи с переносом объекта при помощи квантовой механики. Прослушивание информации при таком способе передачи возможно определить при помощи измерения некоторых определенных параметров физических данных.

Цели — актуальность данной технологической ветки и сферы ее использования на данный момент времени. Описание этапов развития квантовой криптографии.

Методы. В ходе выполнения работы была собрана и проанализирована информация, имеющаяся в открытом доступе от непосредственного открытия квантовой криптографии, до использования ее в настоящее время государствами и частными компаниями. Дальше была произведена сортировка данных и сделан ряд выводов из собранной информации.

Результаты. В июне 2016 г. сотрудники RCC подключились к зданиям Газпромбанка в Москве с помощью квантовой связи. В мае 2017 г. в России специалистам RU удалось создать многоузловую гетерогенную квантовую сеть передачи данных, в которой одновременно использовались два метода кодирования информации. В конце 2017 г. в лаборатории физического факультета МГУ был протестирован работающий квантовый телефон. В августе 2019 г. в структуре компании «Российские железные дороги» был создан департамент квантовых коммуникаций, который будет заниматься развитием соответствующих технологий в России.

В сентябре 2016 г. китайские ученые запустили орбитальный зонд, впоследствии он был успешно использован для первых «межконтинентальных» сеансов квантовой передачи информации. В феврале 2020 г. в США был создан план по созданию квантового интернета. Новый тип Интернета не предназначен для полной замены обычного он будет работать параллельно — как дополнительная защищенная сеть для некоторых областей науки, промышленности и национальной безопасности.

Выводы. В ходе анализа данных было выяснено, что квантовая криптография — не совершенная система защиты шифрования информации. Было доказано, что перехват информации происходит из-за технической отсталости оборудования. Данная проблема была решена, но риски перехвата информации остаются и до сих пор. На данный момент квантовая криптография является молодой наукой, и не известно, каких высот, сможет добиться в будущем. Сейчас разработка квантово-криптографических систем ведется в США, Китае, России и ряде других стран, где Китай лидирует по протяженности квантовой сети.

Ключевые слова: квантовая криптография; квант; квантовая сеть; квантово-криптографическая система; криптография.

Список литературы

1. Голубчиков Д.М., Румянцев К.Е. Квантовая криптография: принципы, протоколы, системы. Таганрог: ТТИ ЮФУ, 2007. 37 с.
2. Молотков С.Н. Квантовая криптография и теоремы В.А. Котельникова об одноразовых ключах и об обсчетах. Доступ по ссылке: http://vak.rutgers.edu/Chapters_T1/010_280%20%D0%A1.%D0%9D.%D0%9C%D0%BE%D0%BB%D0%BE%D1%82%D0%BA%D0%BE%D0%B2%20%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%20%D0%B8%20%D1%82%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D0%B0%20%D0%9A%D0%BE%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0%20%D0%BE%D0%B1%20%D0%BE%D0%B4%D0%BD%D0%BE%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D1%8B%D1%85%20%D0%BA%D0%BB%D1%8E%D1%87%D0%B0%D1%85.pdf

3. Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. Квантовая криптография учебное пособие. Доступ по ссылке: http://sqi.cs.msu.ru/store/storage/ss8dw5n_quantum_cryptography.pdf

Сведения об авторах:

Владимир Константинович Кожеваткин — студент, группа сппи-18; Поволжский государственный университет сервиса, Тольятти, Россия. E-mail: kozhevatkin02@inbox.ru

Владимир Алексеевич Бердников — научный руководитель, доктор экономических наук; Поволжский государственный университет сервиса, Тольятти, Россия. E-mail: berdanka@list.ru