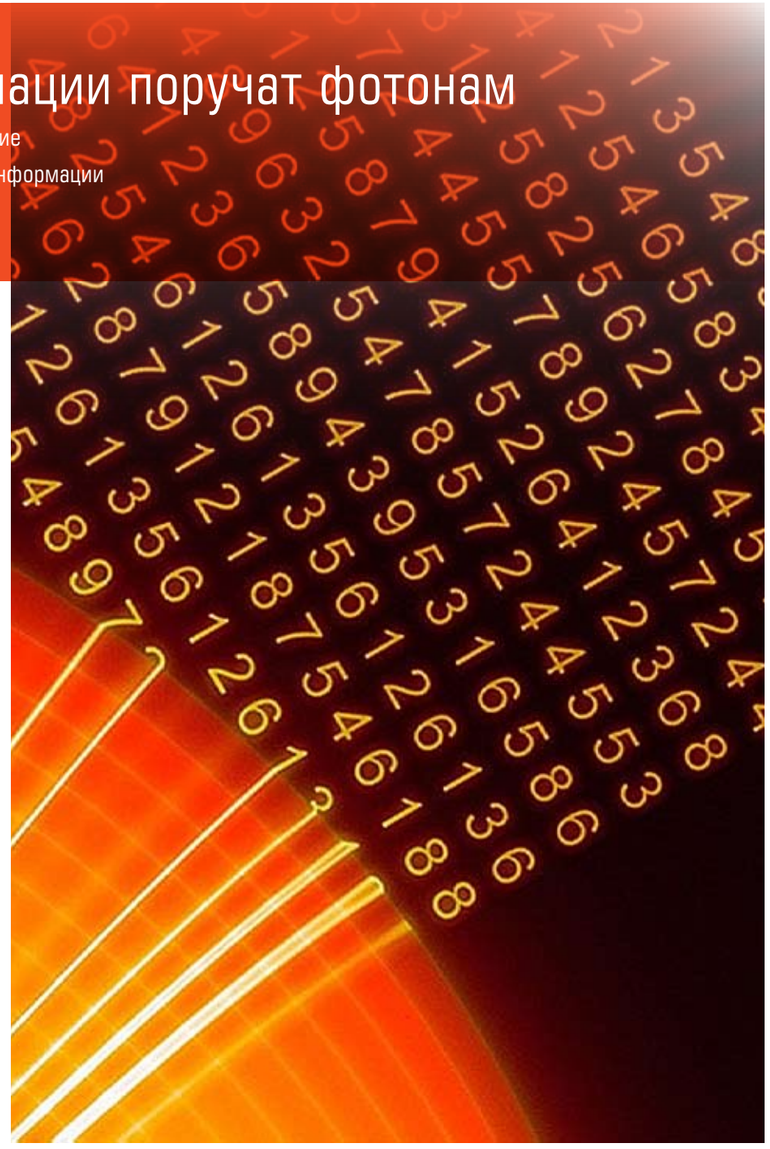
Сергей Куликов

Защиту информации поручат фотонам

Россия пытается сократить отставание от ведущих стран в сфере защиты информации



С начала года было объявлено сразу о нескольких отечественных проектах в отрасли высокотехнологичных методов защиты информации.

«Цифровая экономика базируется на использовании данных, и чем выше стоимость этих данных, тем больше желающих их присвоить, — поясняет директор проектов квантовых коммуникаций компании "Ростелеком" **Сергей Ханенков**. — Кража, утечка, уничтожение данных могут иметь последствия, которые порой страшно представить. Но именно квантовые коммуникации обеспечивают наивысшую из существующих на сегодня степень защиты передачи данных».

Когда случайности не случайны

Квантовый генератор случайных чисел, о разработке которого заявлено учеными НИТУ МИСиС и Российского квантового центра в составе международной исследовательской группы, на сегодня самый быстрый в мире. «Генерация случайных чисел — важнейшая задача для различных областей, таких как криптография или моделирование сложных систем», — говорит один из авторов этого проекта, руководитель научной группы Российского квантового центра и эксперт центра НТИ «Квантовые коммуникации» НИТУ МИСиС **Алексей Федоров**.

Как поясняют разработчики устройства, на первый взгляд сегодня генерируемые компьютером числа могут казаться случайными, но на самом деле предсказать, какое число выдаст машина, во многих случаях все же возможно. А это делает шифры уязвимыми.

Этого можно избежать за счет применения квантового генератора случайных чисел, которые действительно невозможно предсказать. Он передает ключи шифрования через квантовую сеть, созданную для передачи закодированной информации в квантовых состояниях из одной точки в другую. По ней ключи шифрования передаются с помощью одиночных частиц — фотонов. И взломать такую связь незаметно никак не получится, поскольку зашифрованные данные по каналам этой связи передаются только тогда, когда квантово распределенные ключи переданы без ошибок и признаков перехвата. Удобство такой связи еще и в том, что наладить ее можно на уже существующих коммуникациях, главным образом оптоволоконных.

О запуске линии защищенной квантовой телефонии заявил Центр квантовых технологий Московского госуниверситета. Она свяжет между собой 20 абонентских пунктов на территории вуза, а максимальное расстояние между объектами составит 50 километров.

В то же время Центр исследований и разработок компании GS Labs получил патент на способ криптографического преобразования и устройство для его осуществления, позволяющие обеспечить защиту премиального (FHD, UHD) контента в режиме реального времени.

Как пояснил Сергей Ханенков, в прошлом году были завершены разработка и утверждение технического задания по проекту создания квантовой сети между центром обработки данных (ЦОД) «Калининский» и ЦОД Москвы. В этом году компания проведет проектно-изыскательские работы, которые должны определить этапность и сроки строительства. В рамках этого проекта рассматривается возможность использования строящейся магистральной квантовой сети ОАО РЖД на участке Москва — Удомля. «Для нашей компании важно обеспечить сверхнадежную защиту каналов передачи данных между датацентрами, где размещены важнейшие информационные системы, как внутренние, так и внешних заказчиков, в том числе государственные ИТ-системы», — пояснил г-н Ханенков.

Отметим, что отечественные проекты пока меркнут на фоне грандиозного строительства квантовой инфраструктуры в Китае. В начале этого года Университет науки и технологий КНР объявил о пуске первой в мире интегрированной сети квантовой связи протяженностью около 4600 километров, связавшей Пекин и Шанхай через узлы магистральной связи в Цзинане и Хэфее. Причем это уже работоспособный проект: как уточнялось в сообщении китайских ученых, к сети в настоящий момент подключено свыше 150 абонентов, нуждающихся в суперзащищенной связи, — банки, крупные госкорпорации, промышленные предприятия и т. д.

Самые быстрые

«Квантовые генераторы случайных чисел являются неотъемлемым элементом устройств квантовой криптографии (более точно, квантового распределения ключей, КРК), — рассказал Алексей Федоров. — Главное преимущество квантовой криптографии — защищенность информации, гарантированная законами физики».

Созданное под его руководством устройство генерирует случайные числа со скоростью более 8 Гб в секунду, и это рекордный показатель для генераторов подобного типа в мире.

Такая скорость могла бы стать важным козырем в руках российских разработчиков, но проблема в том, что пока в нашей стране все квантовые проекты — экспериментальные.

«Например, в 2016 году Центр квантовых технологий МГУ протестировал в Подмосковье на сетях "Ростелекома" работу системы квантовой криптографии, которая до этого проходила многочисленные проверки в лабораторных условиях», — говорит менеджер отдела развития продуктов компании «ИнфоТеКС» (один из ведущих отечественных производителей программного обеспечения для защиты от компьютерных атак сетей и конечных узлов) **Александр Поздняков**. Тогда в ходе трехнедельного эксперимента обмен сообщениями, зашифрованными с помощью квантовых технологий, был налажен на оптоволоконной линии длиной 32 км между Ногинском и Павловским Посадом. Однако это всего лишь эксперимент, пусть даже и успешный.

«К сожалению, пока в нашей стране крайне мало проектов, которые эксплуатировались бы сколько-нибудь длительное время, сетует г-н Поздняков. — Обычно это происходит следующим образом: ставится экспериментальная задача, привозится оборудование, монтируется, проводится эксперимент, далее оборудование демонтируется. Такой подход удовлетворяет научный интерес, но не дает опыта длительной эксплуатации».

«ИнфоТеКС» начал активно заниматься темой квантовой криптографии еще четыре года назад, когда заключил соглашение с физфаком МГУ, сразу поставив для себя целью создание коммерческих продуктов. «Наше партнерство позволило достаточно быстро создать комплексы квантово-криптографической защиты информации ViPNet Quandor для сетей с топологией "точка–точка" и ViPNet Quantum Security System (QSS) для сетей с топологией "звезда", — поясняет Александр Поздняков. — Хочу отметить, что изготавливается наше оборудование на базе расположенного в России контрактного производства».

Пока квантовое шифрование на экспериментальной стадии, участники развивают уже существующие способы математического шифрования.

Компания GS Labs (Санкт-Петербург) недавно запатентовала свой способ криптографического преобразования (алгоритм S17), который представляет собой расширение существующего алгоритма шифрования AES (Advanced Encryption Standard). Как считает первый заместитель генерального директора компании GS Labs **Максим Самсонов**, сейчас, с развитием рынка цифровых услуг, требуется постоянная модернизация, повышение криптоустойчивости и быстродействия, так что стоять на месте нельзя. «Используя последние достижения российской науки, наша компания в сотрудничестве с СПбГТУ создала уникальную технологию, способную конкурировать с зарубежными, — отмечает г-н Самсонов. — Она интегрируется в микропроцессоры и может быть использована во всех бытовых устройствах, требующих высокого уровня безопасности передачи данных».

Что за щитом

Технологии внедрения квантового распределения ключей очень перспективны, считает Александр Поздняков. «Несмотря на то что она только начала внедряться, со временем ее применение будет возможно практически во всех сферах, — говорит он. — Приведу аналог: информатизация за сравнительно короткое затронула всю человеческую деятельность».

На данный момент ключевые сферы, где необходимо внедрение технологии КРК, связаны с защитой особо важной информации, например персональных и биометрических данных. Но ее можно применять везде, где ценность информации высока, например в банковской сфере.

В IT-инфраструктуре крупных банков есть центры обработки данных, где хранится и резервируется важная информация, в том числе о клиентах и об операциях. Однако при появлении в распоряжении злоумышленников достаточно мощного квантового компьютера данная информация может быть скомпрометирована, если не будет предусмотрена ее соответствующая защита. Впрочем, появление такой угрозы — дело будущего.

«Еще одним практическим примером использования КРК-технологии может быть обновление ключей шифрования в банкоматах, — считает г-н Поздняков. — Традиционно это выполняется вручную доверенным персоналом и напоминает сеанс инкассации. Но при использовании КРК в сети становится возможным обновлять ключи дистанционно, сократив расходы на выезд к каждому банкомату».

Как будем догонять

Над созданием квантово защищенных линий работают все крупные государства. Как отмечает Александр Поздняков, родоначальником строительства квантовых сетей были США, где первая такая сеть появилась в 2001 году. Сейчас лидер на этом направлении — Китай. «В их сети интегрированы сегменты квантового распределения ключей по открытому пространству, — говорит он. — Плюс более 700 оптических сегментов и две станции космической связи с передачей данных по спутниковым каналам. В России такие работы ведутся, но до реализации еще далеко».

Однако, по словам Алексея Федорова, в нашей стране устройства квантовой криптографии внедряются довольно активно, причем разными командами. «Устройства для квантового распределения ключей в России разработали несколько команд. Но при этом говорить, что существует некий разнобой, не совсем правильно. Скорее можно вести речь о здоровой конкуренции среди ученых и разработчиков».

У России есть все возможности для того, чтобы быть среди ведущих держав в этой области. «На старте наших разработок в этой сфере разрыв между нами и мировыми лидерами составлял двадцать лет, сейчас он сократился примерно до пяти лет», — Александр Поздняков. ■