

6. Новиков, М. Ю. Веб-сайт педагога как инструмент профессионального развития / М. Ю. новиков // Международный научно-исследовательский журнал. – 2017. – № 4–3 (58). – С. 42–44.

УДК 003.26:519.728.2:004.7

Соснин А. С.

РАЗВИТИЕ КВАНТОВЫХ СЕТЕЙ И КВАНТОВОЙ КРИПТОГРАФИИ В МИРЕ

Александр Сергеевич Соснин

Студент магистратуры

salexandr18@gmail.com

ФГАОУ ВО «Российский государственный профессионально-педагогический университет», Россия, Екатеринбург

DEVELOPMENT OF QUANTUM NETWORKS AND QUANTUM CRYPTOGRAPHY IN THE WORLD

Aleksandr Sergeevich Sosnin

Russian State Vocation Pedagogical University, Russia, Yekaterinburg

Аннотация. В статье раскрываются основные понятия, принципы работы, этапы развития, и примеры реализации сетей, основанных на квантовых явлениях.

Abstract. The article reveals the basic concepts, principles of work, stages of development, and examples of the implementation of networks based on quantum phenomena.

Ключевые слова: Квантовые сети, квантовая запутанность, история развития в России, квантовая криптография, проблемы реализации.

Keywords: Quantum networks, quantum entanglement, history of development in Russia, quantum cryptography, implementation problems.

Первой работой в области квантовой криптографии, стала работа Стивена Визнера. В 1970 когда Стивен учился в Колумбийском университете, он получил отказ при попытке опубликовать статью по теории кодирования в журнале IEEE Information, по причине того, что описанные в ней предложения посчитали не научными. В этом труде была предложена первая своем роде система, основанная на квантовых состояниях для защиты банковских билетов [1]. Исследователь предложил помещать на билет специальные световые ловушки в каждой из которых помещался фотон с определенной поляризацией. Помимо этого, на билет наносился определенный шифр, который содержал в себе информацию об поляризации каждого из фотонов. При применении фильтра с отличного от заданного, происходило стирание комбинации поляризованных фотонов. Однако состояние развития техники на тот момент исключало применение данной технологии на практике.

Только в 1983 работа Стивена Визнера была опубликована под названием Сопряженное кодирование.

На основе работ Стивена Визнера, специалисты из IBM совместно с учеными Монреальского университета разработали метод кодирования и передачи информации. Разработанный ими протокол получил название BB84 [2] и стал первым протоколом квантовой криптографии. Для кодирования информации применяется протокол, основанный на четырех квантовых состояниях два формирования двух сопряженных базисов.

Параллельно с этим на основе парадокса Эйнштейна — Подольского — Розенберга, а именно на принципе нелокальности спутанных квантовых объектов происходила работа по созданию протокола квантовой криптографии в основе которого лежит эффект спутанных состояний [3].

В 1989 году состоялась первая демонстрация установки распределения квантовых ключей. Процесс передачи происходил через открытую среду на дистанцию около 30 сантиметров [4].

С целью увеличения расстояния передачи информации в качестве среды начали применять оптическое волокно. Первые эксперименты в Женеве показали, что применение оптоволокна в качестве среды позволило увеличить осуществить передачу на дистанцию более 1 километра.

В 1995 году компания British Telecom продемонстрировали передачу на 50 километров. Такая дальность передачи стала возможна благодаря экспериментам с конфигурациями оптических сетей [5].

В 2001 году в Великобритании осуществили передачу на расстоянии 100 километров.

Первый рекорд по достижению максимальной дальности передачи информации был поставлен специалистами Национального института стандартов и технологий и составляет 180 километров [6].

В 2002 году на выставке CeBIT–2002 презентация первой в своем роде коммерческой системы квантовой криптографии разработанной компанией Gar-Optique. Данная установка проставляла собой два небольших 19 дюймовых блоков. В качестве источника фотонов применялся лазер с длинной волны 1559 нм. На основе данной системы была осуществлена связь на расстоянии 67 километров между городами Луизиана и Женева [7].

Активные исследования в области квантовых сетей ведут крупнейшие технологические компании, включая IBM, Mitsubishi, Toshiba, а также авторитетные научные учреждения во всем мире.

Помимо больших компаний стали появляться и небольшие компании, решения которых не уступают в технологичности гигантам. К таким компаниям относятся MagiQ, IdQuantique, Smatr Quantum.

Специалисты из QinetiQ в 2002 осуществили передачу ключа на 24 км через воздушную среду. Для кодирования информации применялась поляризация фотонов [8].

В этом же году специалистами и Северо-западного университета Иллинойс продемонстрировали технологию передачи не только ключа, но шифрованного сообщения. Скорость передачи достигала 250 Мбит/с. Данная работа

была поддержана грантом DARPA в размере 4,7 миллиона долларов. В результате была разработана и запатентована система квантового кодирования AlphaEta [9].

В 2016 году ученые квантового центра Казанского национального исследовательского технического университета (КНИТУ-КАИ) и Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (ИТМО) разработали первую в России многоузловую квантовую сеть. Данная сеть связала два корпуса Казанского университета, расстояние между которыми составила 30 километров [10].

13 декабря 2017 года компания ИнфоТеКс представила защищенный телефон “ViPNet”. Создание данного телефона было основано на интеграции аппаратуры квантового распределения ключей. Данный продукт был создан при участии специалистов Московского государственного университета имени М.В. Ломоносова [11].

В данный момент происходят работы по созданию интегрированных решений систем квантовой связи. Важным критерием для увеличения объема применения данных систем состоит в повышении скорости передачи данных и осуществления передачи в воздушной среде.

На протяжении последних пятидесяти лет, развитие систем квантовой криптографии, прошло путь от полного отрицания возможности реализации данных систем, до теоретических исследований и доказательства основных теорий и создания коммерческих систем, для подачи сообщений на расстояние десятков километров. Также получили развитие системы для передачи информации в воздушной среде. Развитие техники не стоит на месте, разрабатываются новые решения области квантовых сетей. Уже через несколько лет данные сети будут обеспечивать безопасность обмена информацией не только в военных целях, но при совершении банковских операций, и коммуникаций внутри организации. Для создания отечественных аналогов и их повсеместного применения требуется, подготовка широкого диапазона специалистов в этой области. Подготовка специалистов полностью ложится на плечи высших

учебных заведений, так как для работы с данными системами требуются специалисты высокой квалификации. В первую очередь потребуются специалисты в области квантовой физики, систем телекоммуникаций и информационной безопасности.

Список литературы

1. Conjugate coding [Electronic resource]. – URL: [https://www.scirp.org/\(S\(351jmbntvnsjt1aadkposzje\)\)/reference/References_Papers.aspx?ReferenceID=629285](https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/References_Papers.aspx?ReferenceID=629285) (дата обращения: 01.07.2018).
2. Quantum cryptography: Public key distribution and coin tossing [Electronic resource]. – URL: <http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf> (дата обращения: 27.07.2014).
3. Quantum cryptography based on Bell's theorem [Electronic resource]. – URL: <http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf> (дата обращения: 08.02.2019).
4. Experimental quantum cryptography [Electronic resource]. – URL: <https://link.springer.com/article/10.1007/BF00191318> (дата обращения: 08.02.2019).
5. Quantum cryptography on optical fiber networks [Electronic resource]. – URL: <https://www.sciencedirect.com/science/article/pii/S106852009890270X> (дата обращения: 08.02.2019).
6. Long-distance quantum key distribution in optical fiber [Electronic resource]. – URL: <https://iopscience.iop.org/article/10.1088/1367-2630/8/9/193> свободный (дата обращения: 08.02.2019).
7. Quantum key distribution over 67 km with a plug&play system [Electronic resource]. – URL: <https://iopscience.iop.org/article/10.1088/1367-2630/4/1/341/meta> (дата обращения: 08.02.2019).
8. Quantum cryptography: A step towards global key distribution [Electronic resource]. – URL: https://www.researchgate.net/publication/232796734_Quantum_cryptography_A_step_towards_global_key_distribution (дата обращения: 08.02.2019).

9. Quantum-noise randomized data-encryption for WDM fiber-optic networks [Electronic resource]. – URL: https://www.researchgate.net/publication/232796734_Quantum_cryptography_A_step_towards_global_key_distribution (дата обращения: 08.02.2019).

10. Запущена единственная в СНГ многоузловая квантовая сеть [Электронный ресурс]. – Режим доступа: <http://technopark.ifmo.ru/zapushhena-edinstvennaya-v-sng-mnogouzlovaya-kvantovaya-set/> (дата обращения: 08.02. 2019).

11. Квантовый компьютер и квантовая связь [Электронный ресурс]. – Режим доступа: <http://www.tadviser.ru/index.php/> (дата обращения: 08.02.2019).

УДК 004.032.26

Соснин А. С., Сулова И. А.

РЕАЛИЗАЦИЯ ЭЛЕМЕНТАРНОЙ НЕЙРОННОЙ СЕТИ

Александр Сергеевич Соснин

Студент магистратуры

salexandr18@gmail.com

Ирина Александрована Сулова

кандидат педагогических наук, доцент

irina.suslova@rsyru.ru

ФГАОУ ВО «Российский государственный профессионально-педагогический университет», Россия, Екатеринбург

REALIZATION OF ELEMENTARY NEURAL NETWORK

Aleksandr Sergeevich Sosnin

Irina Aleksandrovana Suslova

Russian State Vocation Pedagogical University, Russia, Yekaterinburg

Аннотация. В статье раскрываются реализация нейронной сети и ее последующее обучение.