



НАУЧНЫЙ ЖУРНАЛ НАУКА И МИРОВОЗЗРЕНИЕ

КЛЮЧЕВЫЕ ЗАДАЧИ И ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВРЕМЕННОЙ КВАНТОВОЙ ИНФОРМАТИКИ

Чарыева Дунягозель

преподаватель кафедры Кибербезопасности, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Репова Аннагозель

преподаватель кафедры Кибербезопасности, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Ёмудова Джахан

преподаватель кафедры Кибербезопасности, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Бабаева Реджепбиби

студент Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

В настоящее время квантовая обработка информации в рамках научного направления «Квантовая информатика» отличается значительным потенциалом повышения производительности компьютерно-программных вычислений. Она базируется не на применении традиционной булевой алгебры, а на логических представлениях квантовой механики, которая обеспечивает квантовым компьютерам вычислительную мощность, превышающую на несколько порядков возможности современных классических электронно вычислительных машин, гарантируя при этом безопасность и надежность использования и хранения взаимосвязанных цифровых элементов. Архитектура современных квантовых компьютеров строится не на принципах фон Неймана, а на квантовом параллелизме и квантовой запутанности, что открывает сегодня новые возможности развития ИКТ. Такое положение дел обуславливает актуальность рассмотрения ключевых задач и основных направлений современной квантовой информатики в рамках проблемы применения квантовых вычислений в науке и технике, попытка чего предпринимается в данной работе.

Анализ специальной литературы показывает, что в настоящее время в области квантовой информатики имеется два основных типа задач, которые могут быть эффективно решены с помощью квантовых компьютеров: создание сложных криптографических структур и эмуляция квантовых систем.

Задачи криптографии сегодня базируются на специальных системах шифрования, функционирование которых реализуется путем перемножения больших данных с целью получения шифра, характеризующегося высокими показателями безопасности и

взломостойкости. Здесь наиболее интересной сферой деятельности исследователями принято считать область дешифрования информации, в частности возможность дешифровки. Сегодня безопасность шифров обеспечивается необходимостью длительной и трудоемкой расшифровкой данных. В виду развития особых соответствующих технологий многие современные шифры могут дешифровываться на протяжении тысячелетий. Квантовые же компьютеры, в отличие от традиционных, обладают мощностью, способной раскрывать необходимую информацию в сотни раз быстрее. В ряде случаев на дешифровку шифров квантовые компьютеры затрачивают то же время, за которое был реализован процесс шифрования. В этом контексте огромное множество технологических компаний и банковских организаций в нынешнюю эпоху цифровизации особо заинтересованы в создании, развитии и внедрении квантовых вычислений.

Что касается эмуляции квантовых систем, то исследователи отмечают, что данная область квантовой информатики в настоящее время способна изменить человеческое представление о биологических, химических и физических системах. В рамках квантовой биологии, квантовой химии и физики моделирование наблюдаемых в окружающей среде явлений и процессов обязательный инструмент для разработки инновационных технологий, базирующихся на понимании и техническом приложении объектов и систем естественного мира, а также человеческой культуры. Поскольку устройство последних характеризуется высокой сложностью и огромными объемами информации, обозначенные технологии требуют применения современных технико-технологических решений, в том числе квантовых компьютеров с соответствующими квантовыми вычислениями. Как правило, квантовые компьютеры здесь полезны именно по причине наличия в них двух характерных особенностей: высокая скорость обработки данных и большой объем памяти (как дисковой, так оперативной).

В рамках настоящей работы важным также является краткое рассмотрение современных направлений исследований в сфере квантовой информатики, которые представлены ниже.

1. Квантовая кибербезопасность: умные пространства, безопасное хранение и использование данных

На сегодняшний день учеными в сфере квантовых вычислений комплексно исследована возможность их использования в целях поиска и определения уязвимостей в так называемых умных пространствах. Кибербезопасность в умных пространствах в 2022 году развивается стремительными темпами. Данное технологическое решение более пяти лет входит в десятку наиболее важных цифровых трендов в области надежного хранения и использования информации. Кибербезопасность различных интеллектуальных систем, «умных домов» и «умных городов» открывает возможности упрощения многих привычных для людей действий и функций путем реализации необходимой устойчивости работы цифровой сетевой инфраструктуры. Эксперты прогнозируют, что к 2025 году вопросами кибербезопасности данных в умных пространствах будут обеспокоены более семидесяти пяти процентов крупных и средних компаний по всему миру, поэтому развитие квантовых алгоритмов для выявления уязвимостей и киберзащиты является в настоящее время актуальной проблемой

2. Квантовая криптография

Область современной квантовой криптографии сегодня развивается по пути важности решения практических проблем построения защищенных квантовых сетей, обладающих функциями масштабируемости. Одной из ключевых задач квантово-криптографической

науки является удаленное распространение секретных ключей с помощью внедрения независимых измерительных устройств. Современные технологии с использованием измерений так называемых ненадежных реле позволяют устанавливать секретные ключи между двумя соответствующими сторонами. Усовершенствование последних видится в применении квантовых систем связи, реализованных с помощью сетевых протоколов с когерентным состоянием, которые в количественном аспекте на 2-3 порядка превышают существующие традиционные решения. Квантовые системы связи возможно использовать для создания высокоскоростных криптографических сетей, в которых инновационные устройства могут надежно и безопасно подключаться к ближайшим точкам доступа или прокси-серверам

3. Ключи и алгоритмизация в квантовых системах

Квантовые алгоритмы поиска ключей, их распределение на оптоволокне и анализ квантовых ресурсов, применяющихся в целях осуществления кибератак – важнейшие направления в обозначенном проблемном поле. В настоящее время исследователями активно изучаются вопросы алгоритмических операций, кубитов и эффективности извлечения ключей в квантовых системах. Особое место здесь занимает квантовый алгоритм Гровера, базирующийся на отказоустойчивом логическом наборе квантовых вентилей. Использование последнего в области квантовой кибератаки показывает сегодня высокую эффективность. Если при базовой атаке ключа с блочным шифрованием, киберпреступник получает доступ к шифрам под ключами, отличающимися от целевого бит-флипами, то при квантовой атаке противником запрашивается суперпозиция связанных ключей, после чего они довольно быстро извлекаются. В качестве основной меры противодействия сложным квантовым атакам видится реализация независимого от измеряющего устройства квантового распределения ключей

Таким образом, квантовая информатика является новым научно-техническим направлением, в котором исследуются проблемы использования квантовых объектов для обработки, передачи и хранения цифровой информации. Существует два основных типа задач, которые эффективно решаются с помощью квантовых компьютеров: создание сложных криптографических структур и эмуляция квантовых систем. Современными перспективными направлениями в области квантовых вычислений являются:

- 1) квантовая кибербезопасность: умные пространства, безопасное хранение и использование данных;
- 2) квантовая криптография;
- 3) ключи и алгоритмизация в квантовых системах.