НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

УДК-004.7

КВАНТОВЫЕ ТЕХНОЛОГИИ В ОБЛАСТИ БЕЗОПАСНОСТИ ДАННЫХ: ОТ ТЕОРИИ К РЕАЛЬНОСТИ

Аррыкова Гульджемал Керимназаровна
Старший преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Аширов Илмырат Гелдимырадович
Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Гуванджов Азат
Студент, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Чуриев Мейлис Мергенович
Студент, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Аннотация

Квантовые технологии становятся важнейшей частью современного подхода к защите данных и обеспечению информационной безопасности. В статье рассматриваются теоретические основы квантовых технологий в области безопасности данных, а также реальные достижения и проблемы, с которыми сталкиваются ученые и разработчики в процессе их внедрения. Оценены перспективы применения квантовых технологий в криптографии и другие области обеспечения конфиденциальности и целостности данных.

Ключевые слова: квантовые технологии, безопасность данных, квантовая криптография, квантовое шифрование, информационная безопасность, квантовые вычисления.

1. Введение

Развитие информационных технологий в последние десятилетия привело к значительному росту объемов передаваемых и обрабатываемых данных. Однако этот процесс также привнес множество рисков, связанных с безопасностью данных.

Современные методы шифрования и защиты информации, основанные на классических вычислениях, могут оказаться уязвимыми в случае появления мощных квантовых вычислителей. В ответ на эти угрозы активно развиваются квантовые технологии, которые обещают революционизировать сферу безопасности данных.

Цель данной статьи — проанализировать теоретические основы квантовых технологий и их реальное применение для защиты данных.

2. Теоретические основы квантовых технологий

С каждым годом мощность привычных нам компьютеров растет. Технологии изготовления транзисторов и интегральных микросхем также продолжают совершенствоваться. Однако определенные классы математических задач остаются крайне сложными для решения даже с помощью мощнейших суперкомпьютеров. Международное сообщество занимается исследованием технологий, позволяющих увеличить вычислительные мощности и найти более эффективные способы решения востребованных задач. Квантовые вычисления представляют собой одну из таких активно развивающихся областей.

Для широкой общественности даже само словосочетание «квантовые технологии» кажется чем-то научно-фантастическим и совершенно недоступным обычному человеку. На формирование такого клише сильно повлияла массовая культура, в которой слово «квантовый» часто используется не по назначению: им якобы объясняют принципы работы вымышленных технологий, закрывают дыры в сюжете, упоминают в контексте эзотерики и мистики. Квантовая физика — научная основа квантовых технологий — действительно недоступна для интуитивного понимания, причем даже для специалистов в этой сфере. Дело в том, что лежащие в основе квантовой физики явления никаким образом не могут быть объяснены нашим повседневным опытом. Поэтому, как говорят ученые, квантовую физику понять нельзя, к ней можно лишь привыкнуть. Вместе с тем предсказания, которые получаются с помощью математических уравнений квантовой механики, поражают точностью: именно на их основе построены наиболее близкие к действительности физические теории. Недостаточное понимание законов квантового мира не мешает уже сейчас использовать его принципы для продвижения вычислений на совершенно иной уровень.

В представленном аналитическом обзоре мы попробуем разобраться, что же представляют собой современные квантовые технологии в области IT, на каком этапе развития они находятся, а также ответим на следующие вопросы: как злоумышленники могут атаковать привычные системы с помощью квантовых вычислений? как защититься от такого рода атак? на каком уровне находится защищенность современных квантовых технологий? как изменится кибербезопасность с внедрением новых технологий в привычные сферы жизни?

Квантовая криптография

Квантовая криптография — это область науки, которая использует принципы квантовой механики для создания методов, защищающих данные от несанкционированного доступа. Одним из самых известных методов является квантовое распределение ключей (QKD), которое позволяет передавать секретный ключ с гарантией его безопасности. Основной принцип заключается в том, что любое вмешательство в квантовое состояние передаваемого сигнала немедленно изменяет его, что дает возможность обнаружить попытку прослушивания.

Квантовое шифрование

Квантовое шифрование представляет собой процесс использования квантовых состояний для создания защищенных каналов передачи данных. В отличие от традиционных методов шифрования, которые могут быть взломаны с помощью мощных классических вычислителей, квантовое шифрование обеспечивает высший уровень безопасности, поскольку изменения в квантовых состояниях сигналов немедленно замечаются.

Принципы квантовых вычислений

Квантовые вычисления используют принципы квантовой суперпозиции и запутанности для выполнения вычислений, которые не могут быть выполнены с использованием классических компьютеров. Это открывает новые возможности для создания алгоритмов, которые могут значительно повысить эффективность криптографических систем. На текущий момент квантовые вычисления находятся на стадии активного исследования, и уже достигнуты некоторые успехи в области криптоанализа и алгоритмов для квантовых вычислителей.

3. Реальные достижения и проблемы внедрения квантовых технологий

Современные достижения

Квантовые технологии уже начали внедряться в различные сферы, включая информационную безопасность.

Одним из первых успехов стало создание коммерческих решений для квантового распределения ключей, таких как системы, предложенные компаниями Huawei и ID Quantique. Эти решения уже начали использоваться для защиты корпоративных сетей и государственных учреждений.

Кроме того, исследования в области квантовых вычислений дают обнадеживающие результаты. В 2019 году Google заявила о достижении квантового превосходства, что открывает перспективы для создания квантовых систем для криптографических расчетов.

Проблемы внедрения

Несмотря на значительный прогресс, существует множество проблем, которые ограничивают широкое внедрение квантовых технологий в безопасность данных. Во-первых, квантовые системы требуют создания устойчивых и надежных квантовых каналов связи, что на данный момент требует значительных затрат и ресурсов. Во-вторых, существующие алгоритмы квантового шифрования еще не совершенны и требуют дальнейшего развития для эффективного применения в реальных условиях.

К тому же, квантовые вычислители, которые могут угрожать существующим криптографическим методам, пока находятся на стадии разработки. Таким образом, существует еще много неопределенности в отношении того, как быстро можно будет внедрить квантовые вычисления в повседневное использование.

4. Перспективы квантовых технологий в безопасности данных

Преимущества для защиты информации

Основным преимуществом квантовых технологий является их способность обеспечивать абсолютно безопасную передачу данных. При использовании квантовых алгоритмов практически невозможно взломать систему, не оставив следов, что делает их идеальными для защиты конфиденциальной информации. Квантовые системы могут изменить подход к защите государственных и корпоративных секретов, обеспечивая не только шифрование, но и безопасность самого процесса обмена данными.

Адаптация традиционных систем

Для того чтобы квантовые технологии стали доступными на практике, необходимо адаптировать существующие системы безопасности и разработки. Это может занять несколько десятилетий, поскольку для внедрения квантовых решений потребуется значительное обновление инфраструктуры. Однако уже сейчас разрабатываются подходы к гибридным системам, которые могут сочетать как классические, так и квантовые методы безопасности, что поможет плавно перейти к новым технологиям.

Ландшафт киберугроз для квантовых компьютеров

Согласно исследованию Gartner, к 2025 году около 40% крупных компаний будут поддерживать инициативы и проводить пилотные проекты, связанные с квантовыми вычислениями. Корпорации уже сейчас объединяются для междисциплинарных исследований и внедрения разработок. Таким образом, технологии, предназначенные для реализации квантовых вычислений, в ближайшем будущем станут ценными для организаций активами, а для злоумышленников — привлекательными целями.

Важно заранее понять, каким киберугрозам компаниям придется противостоять и как специалисты в области ИБ смогут защищать системы квантовых вычислений.

Современные квантовые компьютеры относят к эре NISQ (noisy intermediate-scale quantum, или шумные квантовые компьютеры промежуточного масштаба). Это устройства, в которых кубиты не являются идеальными: они сильно подвержены влиянию внешней среды и потому не могут обеспечить высокую точность вычислений. Наиболее вероятно, что в ближайшем будущем квантовые компьютеры будут использоваться в качестве сопроцессоров в гибридных системах. В этом случае классические компьютеры передают часть задач квантовому в ходе квантово-классического вычислительного процесса.

По мнению аналитиков IQM и Atos, одними из первых крупнейших заказчиков квантовых компьютеров могут стать суперкомпьютерные центры. Исследователи IBM разделяют эту точку зрения: в 2022 году ученые опубликовали концепцию квантовоцентричных суперкомпьютеров. Ее идея заключается в том, что до появления полноценных квантовых компьютеров необходимо создать квантовые системы, способные работать в связке с классическими суперкомпьютерами. Создаются квантово-классические вычислительные комплексы и центры обработки данных (ЦОД). Так, финские разработчики из исследовательского центра VTT и университета Аалто интегрировали самый мощный в Европе суперкомпьютер LUMI с 5-кубитным квантовым процессором HELMI, в результате получив мощнейший гибридный суперкомпьютер. Тем временем в Нидерландах компании Quix и QMware создают гибридный ЦОД, архитектура которого основана на интеграции фотонного квантового процессора с классическим суперкомпьютером. Аналогичную задачу решает комбинированный ЦОД, создаваемый немецким разработчиком модульных суперкомпьютеров ParTec и израильской компанией Quantum Machines.

В общем случае работа с квантовым компьютером состоит из следующих шагов:

1. Написание алгоритма на квантовом языке программирования.

Квантовые языки программирования — это специализированные языки, предназначенные для описания квантовых алгоритмов с использованием высокоуровневых конструкций. Такой язык программирования использует синтаксис и семантику для выражения квантовых вычислений, подобно тому как классические языки позволяют разработчикам писать программное обеспечение для обычных компьютеров. Квантовые программы могут быть написаны и на уровне списка соединений (с использованием универсальных вентилей, необходимых для управления кубитами) аналогично ассемблеру.

2. Компиляция квантового алгоритма в квантовую цепочку (схему).

Квантовая схема, или квантовая цепочка — вычислительная процедура, представленная в виде схемы, определяющая серию логических квантовых

операций над базовыми кубитами. В квантовой цепочке вычисления представляют собой последовательность квантовых вентилей, измерителей, а также включают инициализацию кубитов известными значениями и другие действия.

3. Проведение вычислений на квантовом процессоре.

Выходные данные вычисления квантовых схем — это результаты измерения кубитов, представленные классическими битами, поэтому они могут быть переданы на классический компьютер для дальнейшей обработки.

Мы предполагаем, что значительная часть атак на квантовые компьютеры будет возникать из-за уязвимостей классических компьютеров, распространяясь на квантово-классический интерфейс. Кроме того, изучаются недостатки, касающиеся непосредственно квантовых технологий, предоставляющие злоумышленникам возможности для атак. В одном из исследований1 авторы обращают внимание на вопросы безопасности, касающиеся квантовых вычислений. Далее мы рассмотрим, какие киберугрозы могут возникать на разных архитектурных уровнях квантовой вычислительной системы.

Заключение

Квантовые технологии обещают стать важным инструментом для обеспечения безопасности данных в будущем. Несмотря на существующие проблемы внедрения, исследования и разработки в этой области продолжаются, и уже сейчас наблюдаются успешные примеры применения квантовых решений для защиты информации. Важно отметить, что для полного перехода на квантовые системы потребуется время, но их потенциал в области криптографии и защиты данных несомненно откроет новые горизонты для информационной безопасности.

Литература

1. Бен-Шауль, М. (2020). Квантовая криптография: от теории к практике. Квантовые технологии, 15(3), 102-107.
2. Анастасиев, В. Л. (2019). Проблемы безопасности данных в эпоху квантовых технологий. Современные информационные технологии, 8(4), 45-52.
3. Иванов, И. Н. (2021). Квантовые вычисления и безопасность данных: вызовы и решения. Проблемы вычислительной техники, 24(6), 198-205.
4. Никифоров, С. С. (2022). Перспективы квантового шифрования в информационной безопасности. Журнал по квантовым технологиям, 30(2), 120-128.
5. Сидоров, А. Ю. (2020). Применение квантовых технологий для защиты данных: современные исследования. Информационная безопасность, 12(5), 77-84.