# Цифровой щит

## Информационная безопасность в эпоху квантовых вычислений

Артем Демиденко ии

Артем Демиденко

# Цифровой щит: Информационная безопасность в эпоху квантовых вычислений

«Автор»
2025

**Демиденко А.**

Цифровой щит: Информационная безопасность в эпоху квантовых вычислений / А. Демиденко — «Автор», 2025

Цифровой щит: Информационная безопасность в эпоху квантовых вычислений – прорывной труд, который погружает читателя в мир, где квантовые технологии пересекаются с вопросами безопасности информации. Книга предлагает ясное и увлекательное введение в принципы квантовых вычислений, историю развития информационной безопасности и актуальные угрозы, которые они несут. Вы узнаете о квантовой криптографии, революционных алгоритмах и квантостойких системах, способных противостоять новым вызовам. Через призму этических, правовых и экономических аспектов автор раскрывает сложность адаптации бизнеса и общества к новым реальностям. Книга не только информирует, но и вдохновляет на конструктивный диалог о будущем цифровой безопасности. Это обязательное чтение для каждого, кто стремится быть на переднем крае технологических изменений. Обложка: Midjourney - Лицензия.

# Содержание

# Артем Демиденко
# Цифровой щит: Информационная безопасность в эпоху квантовых вычислений

## Введение в мир квантовых вычислений

Квантовые вычисления открывают новые горизонты, одновременно ставя перед человечеством важные задачи и вызовы. Классические вычислительные системы основаны на битах – самых элементарных единицах информации, которые могут принимать значения 0 и 1. Понимание квантовых вычислений начинается с кубита – квантового бита. Кубит способен находиться не только в состояниях 0 и 1, но и в их суперпозиции, что означает, что он может одновременно находиться в обоих состояниях до момента измерения. Принцип суперпозиции дает квантовым компьютерам возможность обрабатывать информацию гораздо быстрее и эффективнее, чем это возможно в классических системах.

Рассмотрим практическое применение этого принципа. Например, задача факторизации больших чисел, лежащая в основе криптографических систем, таких как RSA, требует значительных временных затрат для разложения числа на простые множители. На классических компьютерах решение этой задачи занимает огромное количество времени при увеличении числа разрядов. Квантовые вычисления, используя алгоритм Шора, способны справиться с этой задачей за полиномиальное время, что позволяет значительно сократить время обработки. Этот переход от экспоненциальной временной сложности к полиномиальной не только разрывает основы существующих систем безопасности, но и открывает новые горизонты для методов шифрования.

Помимо суперпозиции, квантовые вычисления используют принцип запутанности – еще одну ключевую концепцию, благодаря которой кубиты могут находиться в взаимосвязанном состоянии. Это свойство позволяет значительно повысить производительность вычислений и разрабатывать новые подходы к передаче информации. Например, использование запутанных кубитов в квантовой криптографии обеспечивает уровень безопасности, недоступный классическим методам. Протоколы, такие как квантовое распределение ключей, защищают от подслушивания, так как любое вмешательство изменяет состояние кубитов, что сразу же становится заметно.

Тем не менее, несмотря на многообещающие перспективы, квантовые вычисления все еще находятся на начальной стадии развития. Операционные системы и архитектуры квантовых машин, такие как IBM Quantum Experience и Google Sycamore, продолжают эволюционировать. На данный момент существующие квантовые компьютеры могут выполнять определенные задачи быстрее, чем их классические аналоги, но они все еще далеки от стабильного функционирования при больших объемах данных. Разработчикам необходимо учитывать эти ограничения и адаптировать свои проекты к новым реалиям, осознавая, что надежность и масштабируемость квантовых решений требуют значительных доработок.

Юристам и специалистам в области безопасности крайне важно понимать, что переход к квантовым вычислениям – это не только вызов, но и возможность. Необходимо повышать квалификацию в области квантовых технологий, следить за новыми исследованиями и активно участвовать в обсуждениях об их использовании. Внедрение квантовых решений

на уровне бизнеса потребует осознания потенциальных рисков и разработки новых методов защиты информации.

Анализируя рынок, стоит отметить, что уже сейчас наблюдается рост числа стартапов и инициатив от крупных компаний, работающих в сфере квантовых технологий. Важно не только изучать теоретическую базу, но и применять на практике квантовые алгоритмы и криптографические меры, что необходимо для обеспечения новых стандартов безопасности.

В заключение, квантовые вычисления представляют собой революцию в мире информационных технологий и безопасности. Успешное пересмотр правил игры, вызванное квантовыми системами, требует постоянного обучения и адаптации. Предпринимателям, разработчикам и специалистам по информационной безопасности следует рассматривать эту технологию не как угрозу, а как возможность для создания новых бизнес-моделей и систем защиты, которые смогут справиться с вызовами будущего. Адаптация к изменениям и своевременное реагирование на новые вызовы станут ключевыми факторами для выживания и успеха на рынке.

# История развития информационной безопасности

Информационная безопасность существует так же долго, как и сам поток информации. С момента появления первых компьютеров и сетей защита данных стала важной задачей. История развития информационной безопасности охватывает множество этапов и технологий, каждая из которых оставила свой след в современных подходах к охране информации.

Начало истории информационной безопасности можно отнести к 1970-м годам, когда первые сети начали соединять компьютеры и обмениваться данными. Одним из первых примеров управления доступом стал проект ARPANET, предшественник Интернета. Простые механизмы проверки подлинности, такие как пароли и контроль доступа на уровне пользователя, появились именно в это время. Реальные проблемы с безопасностью стали очевидны лишь с развитием сетевых технологий и увеличением числа пользователей.

В 1980-х годах нарастали опасения по поводу утечек информации и других киберугроз. В 1983 году были впервые введены термины "информационная безопасность" и "кибербезопасность". В это время такие известные личности, как Рон Ривест и Адриан Ли, предложили различные методы криптографии, включая алгоритм RSA, который обеспечивал защищённый обмен данными. RSA стал отправной точкой для разработки безопасных протоколов связи, таких как SSL и TLS, которые до сих пор являются основой защиты данных в Интернете.

С начала 1990-х ситуация с информационной безопасностью усложнилась. Появление интернета во многом изменило способы кибератак. Трояны, вирусы и черви начали распространяться с нарастающей скоростью. Например, вирус "Morris", выпущенный в 1988 году, заразил около 6000 компьютеров, что составило 10% всех систем на тот момент. Это событие стало предупреждением о возможных масштабах угроз и подчеркнуло важность разработки профессиональных систем безопасности. Однако многие организации продолжали затрачивать минимальные ресурсы на информационную безопасность.

1990-е и 2000-е годы ознаменовались успешной работой первых антивирусных программ и межсетевых экранов. Эффективные антивирусные решения, такие как Norton AntiVirus и McAfee, начали активно использоваться для защиты конечных пользователей. Параллельно началось внедрение концепции "защита от угроз", основанной на поведении угроз, что способствовало формированию более проактивных систем. В это время также начали разрабатываться стандарты информационной безопасности, такие как ISO 27001, нацеленные на управление безопасностью данных на уровне организаций.

С появлением облачных технологий и мобильных устройств в 2010-х годах требования к информационной безопасности стали более сложными и разнообразными. Угрозы стали более изощрёнными, а охрана данных в облаке достигла критической важности. Чтобы гарантировать безопасность, организации начали активно внедрять многофакторную аутентификацию, шифрование данных и управление доступом на основе ролей. Например, компании стали использовать виртуальные частные сети (VPN), чтобы обеспечить безопасный доступ к ресурсам для удалённых сотрудников.

Современные угрозы, такие как DDoS-атаки, фишинг и программы-вымогатели, потребовали новых подходов к безопасности. Многие организации сегодня обращают внимание не только на технологии, но и на создание культуры безопасности. Программы обучения сотрудников, имитирующие реальные фишинговые атаки, стали стандартом для повышения осведомлённости и формирования ментальности безопасности среди пользователей. Кроме того, внедрение практик кибербезопасности на уровне руководства организаций стало необходимым условием для обеспечения устойчивости бизнес-процессов.

Учёные и практики в области безопасности активно занимаются разработкой искусственного интеллекта и машинного обучения, чтобы улучшить механизмы обнаружения угроз. Эти

технологии позволяют не только находить угрозы, но и адаптироваться к ним, обучаясь на основе предыдущих инцидентов. Примеры таких систем можно увидеть в работе платформы Darktrace, которая способна автоматически подстраиваться под новые типы угроз.

В заключение, история развития информационной безопасности многогранна и динамична. Как и в большинстве областей технологий, актуальность безопасности информации продолжает меняться в зависимости от окружающей среды и новых технологических изменений. Применение комплексных подходов – от технических решений до повышения осведомлённости – а также адаптация к новым вызовам, таким как квантовые вычисления, будут определять будущие стратегии защиты информации. Инвестиции в обучение сотрудников и регулярные обновления технологий будут ключевыми факторами в поддержании безопасности в условиях быстро меняющегося цифрового мира.

# Основы квантовых вычислений и их особенности

Квантовые вычисления – это область, которая соединяет в себе элементы квантовой механики и теории вычислений, создавая новую парадигму обработки данных. В отличие от классических систем, которые работают с битами, квантовые системы функционируют на основе кубитов – математических объектов, способных находиться в состоянии суперпозиции и запутанности. Понимание этих свойств является ключом к осмыслению преимуществ и сложностей, которые приносит квантовая вычислительная техника.

Суперпозиция кубитов позволяет обрабатывать информацию параллельно. Например, в классическом компьютере для вычислений с двумя битами потребуется время, пропорциональное количеству операций. Однако в квантовом компьютере два кубита могут одновременно представлять четыре состояния (00, 01, 10, 11), что приводит к резкому увеличению вычислительных мощностей. Ярким примером практического применения этого эффекта является алгоритм Шора, который способен факторизовать большие числа за полиномиальное время, в отличие от экспоненциального времени, необходимого для классических алгоритмов. Таким образом, квантовые вычисления могут существенно ускорить задачи, связанные с криптографией, оптимизацией и моделированием.

Еще одной важной концепцией в квантовых вычислениях является запутанность. Это явление описывает, как состояние одного кубита может зависеть от состояния другого, даже если они находятся на большом расстоянии друг от друга. Запутанные кубиты активно применяются в квантовой криптографии, где их используют для реализации протоколов, таких как квантовая распределенная генерация ключей. Даже малейшие изменения в состоянии одного из кубитов немедленно сказываются на состоянии другого, что обеспечивает высокий уровень безопасности передачи данных. Протокол BB84 – один из известных примеров, использующих запутанность.

Квантовые компьютеры также основаны на принципах интерференции. Этот феномен позволяет выделять нужные результаты из множества возможных выходных данных, полученных благодаря суперпозиции. Алгоритм Гровера наглядно демонстрирует, как можно значительно ускорить поиск в неструктурированных базах данных. Вместо того чтобы просматривать каждую запись по очереди, квантовый алгоритм использует интерференцию для увеличения вероятности нахождения решения. Это особенно важно при работе с большими объемами данных, как в биомедицинских исследованиях или финансовом анализе.

Несмотря на свои преимущества, квантовые вычисления сталкиваются с рядом технических проблем. Одна из главных – защита кубитов от декогеренции, когда кубиты теряют свои квантовые свойства из-за взаимодействия с внешней средой, что приводит к потере информации. Современные исследователи и инженеры разрабатывают новые методы коррекции ошибок и защиты кубитов от этого воздействия. Например, метод кодирования Торано используется для создания устойчивых к ошибкам квантовых систем, что значительно повышает надежность квантовых вычислений.

Для более глубокого внедрения квантовых вычислений в бизнес-процессы важно учитывать реальные случаи их применения. Финансовый сектор активно исследует алгоритмы для ускорения депозитных операций или моделирования рынка. Например, банки могут использовать квантовые алгоритмы для оптимизации портфеля активов или оценки инвестиционных рисков. Применение квантовых технологий уже сейчас позволяет существенно улучшить качество предсказаний и анализа данных.

В будущем ожидается, что рост доступности квантовых вычислений изменит стандарты безопасности в отрасли. Чтобы подготовиться к этому переходу, организациям важно начать внедрять квантово-устойчивые алгоритмы шифрования. К таким алгоритмам отно-

сятся, например, алгоритмы на основе решеток, которые, как предполагается, смогут противостоять атакам квантовых компьютеров. Разработка и тестирование таких решений становятся неотъемлемой частью стратегии информационной безопасности.

В заключение, основы квантовых вычислений и их особенности создают новую базу для революционных изменений в различных областях. Понимание принципов суперпозиции, запутанности и интерференции, а также готовность адаптироваться к новым вызовам, предоставит конкурентные преимущества организациям уже сегодня. Используя возможности квантовых вычислений, можно не только оптимизировать текущие процессы, но и заложить стратегическое основание для будущего в эпоху квантовых технологий.

# Квантовая криптография: новая эпоха шифрования

Квантовая криптография – это революционный подход к защите информации, который использует принципы квантовой механики для создания абсолютно безопасных каналов связи. В отличие от традиционных методов шифрования, таких как RSA и AES, которые обеспечивают безопасность только при определённых условиях вычислительной сложности, квантовая криптография предлагает защиту на основе законов физики. В этой главе мы обсудим, как работает квантовая криптография, её преимущества и недостатки, а также её практическое применение.

**Принципы квантовой криптографии**

Основополагающим принципом квантовой криптографии является использование квантовых битов, или кубитов, для передачи информации. Самым известным протоколом, реализующим этот принцип, является протокол квантового распределения ключей, разработанный Чарльзом Беннетом и Жаном-Себастьяном Брюссаром в 1984 году. Этот протокол позволяет двум сторонам, которых обычно называют Алисой и Бобом, генерировать и обмениваться секретным ключом.

QKD работает благодаря уникальным свойствам кубитов: любое измерение кубита изменяет его состояние, что позволяет обнаруживать попытки перехвата информации. Например, если злоумышленник, условно назовём его Эвой, попытается скопировать состояние кубита, это приведёт к изменению передаваемых данных, что немедленно станет известным Алисе и Бобу. Таким образом, если во время передачи обнаруживается какая-либо аномалия, стороны могут отказаться от использования скомпрометированного ключа.

**Преимущества квантовой криптографии**

К основным преимуществам квантовой криптографии следует отнести её способность гарантировать абсолютную безопасность. Поскольку любые попытки перехвата данных автоматически меняют состояние передаваемой информации, пользователи могут быть уверены, что их обмен не был подслушан. Это делает квантовую криптографию особенно важной для таких ключевых сфер, как банковские услуги, государственные структуры и защитные технологии.

Кроме того, квантовая криптография позволяет создавать ключи, которые невозможно вычислить или предсказать. Даже самые мощные квантовые компьютеры, которые могут эффективно решать задачи классического шифрования, не смогут восстановить или повторно использовать секретный ключ. Исследования показывают, что использование квантовых ключей создаёт систему, способную противостоять как классическим, так и квантовым атакам благодаря своей основной структуре.

**Ограничения и вызовы**

Несмотря на явные преимущества, квантовой криптографии пока присущи серьёзные ограничения. Во-первых, для реализации QKD необходима высокотехнологичная инфраструктура, что может значительно увеличить затраты на внедрение и содержание системы. Использование квантовых каналов требует специального оборудования, например, лазеров и фотонных детекторов, что затрудняет массовое применение этой технологии.

Во-вторых, длина квантового канала ограничена, поскольку передача кубитов через оптические волокна ухудшает их состояние на больших расстояниях. Существующие системы QKD могут надежно работать на расстояниях до 100 км, после чего потери сигнала затрудняют гарантирование безопасности шифрования. Разработка рекуперационных сетей и новых технологий передачи остаётся актуальной задачей для будущего квантовой криптографии.

**Практическое применение и примеры**

По последним данным, квантовая криптография всё больше находит применение в финансовом секторе. Некоторые банки уже испытывают систему QKD для защиты своих коммуникаций и обеспечения безопасности конфиденциальных данных клиентов. Например, в 2020 году Банковский союз Швейцарии успешно протестировал установку, способную передавать квантовые ключи между отделениями в различных городах, что подтвердило её эффективность в реальных условиях.

Другим примером является проект «Квантовая сеть Мюнхена», который объединил несколько узлов через сеть оптического волокна, демонстрируя возможность передачи информации с использованием QKD. В будущем создание таких сетей обещает значительно повысить безопасность корпоративной связи и защиту деликатных данных.

**Заключение**

Квантовая криптография представляет собой важный элемент в развитии информационной безопасности, открывая новые горизонты для защиты данных в эпоху квантовых вычислений. Несмотря на свои ограничения, технологии QKD продолжают развиваться и внедряться в разные сферы, что поможет повысить уровень безопасности в условиях быстроменяющихся угроз и вызовов. Следующим шагом станет интеграция квантовой криптографии в уже существующие системы защиты данных, что обеспечит надёжность и безопасность в цифровом мире.

# Квантовые алгоритмы и их влияние на безопасность

Квантовые алгоритмы – это группа инструкций, основанных на принципах квантовой механики, которые способны решать определённые задачи намного быстрее, чем привычные алгоритмы на классических компьютерах. Это стремительное развитие математических концепций связано с их потенциальным влиянием на безопасность данных и шифрование. Существует мнение, что некоторые текущие методы криптографии могут стать неэффективными, если квантовые компьютеры смогут полностью реализовать свои возможности. В этой главе мы рассмотрим ключевые квантовые алгоритмы, их внутренние механизмы, а также влияние на современную информационную безопасность.

Одним из самых известных квантовых алгоритмов является алгоритм Шора, созданный в 1994 году. Он способен эффективно разлагать большие числа на множители, что представляет собой серьёзную угрозу для традиционной системы шифрования RSA, основанной на сложности разложения. Алгоритм использует методы квантовой суперпозиции и интерференции для поиска периодичности, что позволяет существенно сократить время вычислений. Классический подход требует экспоненциальных затрат времени на разложение больших чисел, в то время как алгоритм Шора справляется с этой задачей за полиномиальное время. Этот прорыв побудил индустрию активно заниматься исследованиями в области устойчивых к квантовым вычислениям методов шифрования.

Следующим значимым квантовым алгоритмом является алгоритм Гровера, предназначенный для поиска по неструктурированным данным. Он может решать задачи, которые требуют перебора всех возможных значений, вдвое быстрее, чем лучшие известные классические алгоритмы. Например, для поиска элемента в неупорядоченном массиве из N элементов классическому алгоритму в среднем потребуется N/2 операций, в то время как алгоритму Гровера понадобится всего $\sqrt{N}$ операций. Это ускорение имеет серьёзные последствия для систем, использующих различные способы доступа к данным, и может значительно ослабить безопасность систем, основанных на классических методах поиска.

Чтобы противостоять этим вызовам, информационной безопасности необходимо сосредоточиться на разработке квантово-устойчивых алгоритмов. Новые криптографические протоколы и алгоритмы, такие как методы кодирования на основе кода Гифорда или алгоритмы, использующие решетки, могут гарантировать достаточный уровень безопасности для защиты от атак квантовых компьютеров. Исследования по созданию и улучшению таких алгоритмов активизировались, так как многие учёные понимают необходимость разработки устойчивых к квантовым атакам систем, пока квантовые компьютеры ещё не стали повсеместными.

Однако в кибербезопасности, как в совокупности процессов и технологий, помимо создания новых алгоритмов, требуется также обновление в области образования и организации. Важно учитывать множество аспектов. Образование в области квантовых технологий должно внедряться на уровне учебных заведений и специализированных курсов. Специалисты по кибербезопасности и разработчики должны получать новые знания, чтобы соответствовать современным стандартам безопасности. Кроме технического образования, организациям следует развивать стратегический подход к внедрению квантовых решений, вовлекая в этот процесс все уровни, включая руководство и сотрудников.

В заключение, современные квантовые алгоритмы способны преобразовать подход к безопасности данных, как с использованием традиционных методов, так и с созданием новых стандартов в криптографии. Адаптация к этим изменениям должна стать приоритетной задачей не только для специалистов в области кибербезопасности, но и для всех, чьи интересы затрагивают безопасность информации – от разработчиков программного обеспечения до руководителей компаний. Настало время принять вызов квантового века и разработать системы,

устойчивые к атакам, способные противостоять искусственному интеллекту, который определит следующий этап в эволюции вычислений и безопасности.

# Угрозы информационной безопасности в квантовый век

Квантовые вычисления обещают радикальные изменения в нашем мире. Но наряду с новыми возможностями появляются и серьезные угрозы для информационной безопасности. В этой главе мы рассмотрим основные риски, которые могут возникнуть в эпоху квантовых вычислений, и предложим методы бороться с этими вызовами.

Первая и наиболее серьезная угроза заключается в способности квантовых компьютеров взламывать традиционные криптографические системы. Алгоритмы, такие как RSA и ECC, основанные на сложности разложения больших чисел и вычисления дискретных логарифмов, могут оказаться уязвимыми перед алгоритмом Шора. Этот алгоритм способен за полиномиальное время находить секретные ключи, защищающие информацию, что делает практически невозможным использование существующих методов криптографии для её защиты. Это означает, что данные, зашифрованные по современным стандартам до появления квантовых машин, могут быть вскрыты в будущем, когда мощные квантовые компьютеры станут реальностью.

Второй угрозой является атака с использованием квантовой запутанности. Представим, что злоумышленник создаёт кубиты в состоянии запутанности с законными пользователями и использует это для перехвата и изменения сообщений, передаваемых по каналу. Эта форма атаки, известная как "атака с использованием промежуточной запутанности", может быть весьма трудноразличимой, так как нарушает привычные правила передачи информации при использовании классических методов шифрования.

Третья угроза называется "временная угроза" или "угроза хранения". Согласно этой концепции, злоумышленники могут перехватывать зашифрованные данные и хранить их до тех пор, пока квантовые компьютеры не достигнут необходимого уровня развития, чтобы успешно расшифровать такую информацию. Этот подход стал возможен благодаря квантовым вычислениям, ведь даже самые защищённые методы шифрования могут оказаться под угрозой в будущем. Поэтому важно заранее задуматься о стойкости хранения данных, используя методы постквантовой криптографии.

Четвёртая угроза связана с возможными атаками на сети и каналы передачи данных. Традиционные методы сетевой безопасности, такие как VPN и SSL, могут оказаться уязвимыми перед мощными квантовыми системами. Например, несмотря на то, что обычная аутентификация с использованием паролей и сертификатов защищена от многих видов атак, квантовые угрозы могут снизить её надёжность. Рекомендуется применять методы зашифрованной аутентификации, основанные на криптографических системах, устойчивых к квантовым вычислениям, таких как алгоритмы, построенные на решётках или аналогах.

Для организаций, работающих в условиях квантовых угроз, важно на ранних стадиях внедрять постквантовые криптографические алгоритмы. К таким алгоритмам относятся криптография на основе кодов, мясорубок и многочленов. Эффективная стратегия обновления безопасности должна включать регулярный аудит используемых криптографических систем и планы перехода на современные методы защиты.

Кроме того, необходимо повышать осведомлённость работников о киберугрозах, связанных с квантовыми вычислениями. Обучение сотрудников основам квантовой криптографии и информации о потенциальных рисках поможет достичь более высокого уровня защиты данных и осознания возможных уязвимостей.

В заключение, хотя квантовые вычисления открывают множество возможностей, они также представляют новые риски для кибербезопасности. К этим угрозам нужно подходить с

умом, применяя стратегии, способные адаптироваться к быстро меняющейся технологической среде. Осознание возможных рисков и внедрение постквантовых методов уже сегодня станут важными шагами на пути к обеспечению надёжной информационной безопасности в эпоху квантовых вычислений.

# Проблемы существующих криптосистем перед квантовыми угрозами

С переходом в эпоху квантовых вычислений возникает необходимость пересмотра и анализа надежности существующих криптографических систем. Современные алгоритмы шифрования, такие как RSA и алгоритмы на основе эллиптических кривых, были разработаны для защиты информации в условиях ограниченных вычислительных мощностей классических компьютеров. Однако с появлением квантовых алгоритмов, таких как алгоритм Шора, которые способны эффективно решать задачи, в которых заключается безопасность этих систем, актуальность пересмотра значительно возрастает.

Прежде всего, стоит обратить внимание на алгоритм RSA, который основан на факторизации больших чисел. Его безопасность зависит от сложности разложения произвольного числа на множители. Но алгоритм Шора может найти делители числа значительно быстрее, чем любые известные классические методы. Например, для числа в 2048 бит классическим методам может потребоваться десятки лет на факторизацию, тогда как квантовый компьютер, использующий алгоритм Шора, решит эту задачу всего за несколько минут. Это изменит всю концепцию безопасности: любой, кто обладает квантовым компьютером, сможет легко взломать большинство существующих систем шифрования, что делает защиту информации всё более сложной задачей.

Другой важный криптографический алгоритм – это алгоритм на основе эллиптических кривых. Благодаря высокой степени безопасности при относительно небольших ключах, его часто используют в мобильных устройствах и для защиты интернет-трафика. Однако и здесь существует угроза. Хотя алгоритм Шора напрямую не применяется к алгоритму на основе эллиптических кривых, его способности могут поставить под сомнение безопасность схем, основанных на сложных задачах, таких как дискретный логарифм. В этой связи необходимо разработать стратегии перехода на более безопасные подходы, например, алгоритмы на основе решеток, которые пока не подвержены известным квантовым атакам.

Создание новых криптографических решений – это не только вопрос защиты данных, но и вопрос времени. Многие организации должны хранить зашифрованную информацию в течение многих лет, чтобы соответствовать требованиям законодательства. Существующие алгоритмы, такие как стандарт шифрования AES, по-прежнему обеспечивают безопасность в условиях текущих угроз, но как только квантовые компьютеры станут широко доступными, шифрование с использованием AES окажется уязвимым перед алгоритмами вроде алгоритма Гровера. Этот алгоритм может сократить «долговечность» 256-битного ключа до 128 бит, что уже представляет собой значительную угрозу для защиты информации. Для повышения безопасности рекомендуется использовать ключи большего размера, например, перейти на 512-битное шифрование.

К тому же, постквантовая криптография становится активно развивающейся областью исследований. Стоит рассмотреть внедрение алгоритмов, таких как NTRU, которые способны находить оптимальные решения для шифрования в новых условиях. Эти методы не основаны на традиционных математических сложностях, которые угрожают существующим системам, и предполагают использование различных математических структур, что делает их более стойкими к квантовым атакам.

# Конец ознакомительного фрагмента.