ОСНОВЫ WEB ПРОГРАММИРОВАНИЯ

02.03.03 -Математическое обеспечение и администрирование информационных систем, направленность (профиль) -разработка и администрирование информационных систем

http//vikchas.ru

Лекция 10. «**Квантовый компьютер и WEB-среда Интернет**»

Часовских Виктор Петрович
доктор технических наук, профессор кафедры
ШИиКМ, ФГБОУ ВО «Уральский государственный
экономический университет

Екатеринбург 2026

1. Введение

Современный Интернет и WEB-среда стали основой информационного общества. Через веб-сайты, облачные сервисы, социальные сети, поисковые системы и онлайн-платформы ежедневно передаются огромные объёмы данных. Одновременно с этим развивается новая вычислительная технология — **квантовые компьютеры**.

Квантовый компьютер — это устройство, использующее законы квантовой механики для обработки информации. В отличие от классического компьютера, который работает с битами, квантовый компьютер использует **кубиты**. Это открывает новые возможности для вычислений, криптографии, моделирования сложных систем и развития будущих интернет-технологий.

2. Классический компьютер и Интернет

Классический компьютер обрабатывает информацию в виде битов. Бит может принимать одно из двух значений:

- 0
- 1

Все данные в Интернете — текст, изображения, видео, звук, программы — в конечном счёте представлены в виде последовательностей нулей и единиц.

WEB-среда Интернет включает:

- сайты и веб-приложения;
- браузеры;
- серверы;
- поисковые системы;
- облачные хранилища;
- базы данных;
- протоколы передачи данных, например HTTP и HTTPS.

Классические компьютеры и серверы обеспечивают работу всей современной сети Интернет.

3. Что такое квантовый компьютер

Квантовый компьютер — это вычислительная система, использующая квантовые свойства частиц: электронов, фотонов, ионов или сверхпроводящих цепей.

Главная единица информации в квантовом компьютере — **кубит**.

Если обычный бит может быть либо 0, либо 1, то кубит может находиться в состоянии, которое называется **суперпозицией**. Это означает, что он как бы сочетает в себе состояния 0 и 1 одновременно до момента измерения.

Кроме суперпозиции, квантовые компьютеры используют ещё одно важное явление — **квантовую запутанность**. Запутанные кубиты связаны между собой таким образом, что изменение состояния одного кубита влияет на состояние другого, даже если они находятся на расстоянии.

4. Основные принципы квантовых вычислений

4.1. Суперпозиция

Суперпозиция позволяет квантовой системе одновременно находиться в нескольких состояниях. Благодаря этому квантовый компьютер может обрабатывать большое количество вариантов одновременно.

4.2. Запутанность

Квантовая запутанность позволяет создавать сильные связи между кубитами. Это даёт возможность выполнять вычисления, которые сложно или практически невозможно эффективно выполнить на классическом компьютере.

4.3. Интерференция

Интерференция используется для усиления правильных ответов и ослабления неправильных. Квантовые алгоритмы строятся так, чтобы вероятность получения верного результата была максимальной.

5. Возможности квантовых компьютеров

Квантовые компьютеры не являются просто «более быстрыми» версиями обычных компьютеров. Они эффективны не для всех задач, а только для определённых классов проблем.

Основные области применения:

1. **Криптография**
    - Взлом некоторых современных методов шифрования.

    - Создание новых методов защиты данных.
2. **Моделирование молекул и материалов**
    - Разработка лекарств.
    - Создание новых материалов.
    - Исследование химических реакций.
3. **Оптимизационные задачи**
    - Логистика.
    - Планирование маршрутов.
    - Управление производством.
4. **Искусственный интеллект**
    - Ускорение некоторых методов машинного обучения.
    - Анализ больших данных.
5. **Финансовое моделирование**
    - Оценка рисков.
    - Оптимизация инвестиционных портфелей.

6. Квантовый компьютер и безопасность Интернета

Одним из самых важных вопросов является влияние квантовых компьютеров на безопасность WEB-среды.

Современный Интернет широко использует шифрование. Например, протокол HTTPS защищает данные между браузером и сервером. Для защиты применяются криптографические алгоритмы:

- RSA;
- Diffie–Hellman;
- ECC — криптография на эллиптических кривых.

Эти алгоритмы считаются надёжными для классических компьютеров, потому что их взлом требует огромных вычислительных ресурсов. Однако мощный квантовый компьютер с алгоритмом Шора сможет эффективно решать задачи факторизации больших чисел и дискретного логарифмирования. Это может поставить под угрозу современные системы шифрования.

Постквантовая криптография

Чтобы подготовиться к будущему, развивается **постквантовая криптография**. Это методы шифрования, устойчивые к атакам квантовых компьютеров.

Постквантовые алгоритмы основаны на задачах, которые считаются сложными как для классических, так и для квантовых компьютеров, например:

- решётчатая криптография;
- хэш-based подписи;
- кодовая криптография;
- многомерные квадратичные уравнения.

Переход на постквантовые алгоритмы — одна из важных задач развития безопасного Интернета.

7. Квантовый Интернет

Кроме квантовых компьютеров, развивается идея **квантового Интернета**.

Квантовый Интернет — это сеть, в которой информация передаётся с использованием квантовых состояний. Он не заменит полностью современный Интернет, но может стать его важным дополнением.

Возможности квантового Интернета:

- сверхзащищённая передача ключей шифрования;
- объединение квантовых компьютеров в сеть;
- распределённые квантовые вычисления;
- квантовая телепортация состояний;
- новые методы синхронизации и связи.

Важно понимать, что квантовая телепортация не означает мгновенную передачу предметов или людей. Это передача квантового состояния от одной системы к другой при помощи запутанности и классического канала связи.

8. Квантовое распределение ключей

Одним из практических направлений является **квантовое распределение ключей** — QKD.

QKD позволяет двум сторонам создать общий секретный ключ. Если злоумышленник попытается перехватить квантовые частицы, состояние системы изменится, и факт вмешательства будет обнаружен.

Пример известного протокола — **BB84**.

Преимущество QKD заключается в том, что его безопасность основана на законах физики, а не только на сложности математических задач.

Однако у QKD есть ограничения:

- высокая стоимость оборудования;
- ограниченная дальность передачи;
- необходимость специализированной инфраструктуры;
- сложность интеграции с существующим Интернетом.

9. Квантовые облачные сервисы

Сегодня доступ к квантовым компьютерам часто предоставляется через Интернет. Это называется **квантовые облачные вычисления**.

Пользователь может подключиться к квантовому процессору через веб-интерфейс или API и запускать квантовые алгоритмы удалённо.

Примеры платформ:

- IBM Quantum;
- Google Quantum AI;
- Microsoft Azure Quantum;
- Amazon Braket;
- D-Wave Leap.

Такой подход делает квантовые технологии доступными для студентов, исследователей и разработчиков без необходимости иметь собственный квантовый компьютер.

10. WEB-среда и квантовые технологии

WEB-среда Интернет может взаимодействовать с квантовыми технологиями несколькими способами:

1. **Доступ к квантовым вычислениям через браузер**

    - Пользователь запускает квантовые программы онлайн.
2. **Облачные API**
    - Разработчики используют квантовые процессоры как удалённые вычислительные ресурсы.
3. **Защита веб-сервисов**
    - Внедрение постквантового шифрования в HTTPS и VPN.
4. **Образовательные платформы**
    - Онлайн-курсы, симуляторы квантовых схем, интерактивные лаборатории.
5. **Научные вычисления**
    - Совместная работа исследователей через веб-платформы.

11. Проблемы развития квантовых компьютеров

Несмотря на большие перспективы, квантовые компьютеры пока находятся на стадии активного развития.

Основные проблемы:

- нестабильность кубитов;
- ошибки при вычислениях;
- необходимость сверхнизких температур;
- сложность масштабирования;
- высокая стоимость оборудования;
- ограниченное количество кубитов;
- необходимость квантовой коррекции ошибок.

Кубиты очень чувствительны к внешним воздействиям. Любой шум может привести к потере квантового состояния — это называется **декогеренцией**.

12. Влияние квантовых технологий на будущее Интернета

Квантовые технологии могут значительно изменить Интернет в будущем:

- усилить защиту данных;
- изменить стандарты шифрования;

- создать новые сетевые архитектуры;
- обеспечить безопасную передачу информации;
- ускорить обработку отдельных типов задач;
- позволить создавать распределённые квантовые вычислительные системы.

Однако в ближайшее время квантовые компьютеры не заменят классические компьютеры. Скорее всего, они будут использоваться совместно: классические системы будут управлять данными, интерфейсами и сетью, а квантовые — решать специальные вычислительные задачи.

13. Заключение

Квантовый компьютер и WEB-среда Интернет — это две важные области современных информационных технологий. Квантовые компьютеры способны решать некоторые задачи намного эффективнее классических машин, а Интернет предоставляет удобную среду для доступа к этим ресурсам.

Главное влияние квантовых технологий на Интернет связано с безопасностью данных, развитием постквантовой криптографии, квантовым распределением ключей и созданием квантового Интернета.

Будущее, вероятно, будет гибридным: классический Интернет сохранит свою основную роль, но в него постепенно будут внедряться квантовые методы защиты, связи и вычислений.

Краткие выводы

1. Квантовый компьютер использует кубиты вместо обычных битов.
2. Кубиты могут находиться в суперпозиции и быть запутанными.
3. Квантовые компьютеры перспективны для криптографии, химии, оптимизации и моделирования.
4. Мощные квантовые компьютеры могут угрожать современному шифрованию Интернета.
5. Для защиты разрабатывается постквантовая криптография.
6. Квантовый Интернет может обеспечить новые способы безопасной связи.

7. Доступ к квантовым компьютерам уже возможен через WEB-среду и облачные платформы.