11. Перспективы развития ВТ. Квантовые компьютеры.

Квантовый компьютер — вычислительное устройство, работающее на основе квантовой механики. Квантовый компьютер принципиально отличается от классических компьютеров, работающих на основе классической механики.

Полноценный квантовый компьютер является пока гипотетическим устройством, сама возможность построения которого связана с серьёзным развитием квантовой теории в области многих частиц и сложных экспериментов; эта работа лежит на переднем крае современной физики.

Упрощённая схема вычисления на квантовом компьютере выглядит так: берётся система кубитов, на которой записывается начальное состояние. Затем состояние системы или её подсистем изменяется посредством унитарных преобразований, выполняющих те или иные логические операции. В конце измеряется значение, и это результат работы компьютера. Роль проводов классического компьютера играют кубиты, а роль логических блоков классического компьютера играют унитарные преобразования.

Куби́т (q-бит, кьюбит, кубит; от quantum bit) — квантовый разряд или наименьший элемент для хранения информации в квантовом компьютере.

Унитарные операции: в квантовой механике состояние квантовой системы описывается вектором в гильбертовом пространстве. Норма вектора состояния изолированной квантовой системы описывает вероятность найти систему хоть в каком-либо состоянии, а значит, она обязана равняться единице. Соответственно, эволюция квантовой системы во времени — это некоторый оператор, зависящий от времени, и, из-за требования сохранения нормы, он является унитарным. Неунитарные операторы эволюции для изолированной квантовой системы запрещены в квантовой механике.

Чем же квантовый компьютер лучше классического? Большая часть современных ЭВМ работают по такой же схеме: n бит памяти хранят состояние и каждый такт времени изменяются процессором. В квантовом случае система из n кубитов находится в состоянии, являющимся суперпозицией всех базовых состояний, поэтому изменение системы касается всех 2^n базовых состояний одновременно. Теоретически новая схема может работать намного (в экспоненциальное число раз) быстрее классической.

Агентство национальной безопасности (АНБ) США внедряет средства сбора информации в вычислительную технику и оборудование связи. Однако этим спецслужба не ограничивается. Согласно публикации источника, в экранированных лабораториях АНБ кипит работа по созданию квантового компьютера, который сможет взломать большинство шифров, защищающих банковские, медицинские, коммерческие и правительственные секреты по всему миру.

Источником сведений для публикации стали документы, полученные от бывшего сотрудника АНБ Эдварда Сноудена. В них сказано, что попытки создать «криптографически полезный квантовый компьютер», экспоненциально превосходящий классические компьютеры по производительности, являются частью исследовательской программы под названием Penetrating Hard Targets, что можно примерно перевести как «Проникновение к хорошо защищенным целям». Бюджет программы примерно равен 80 млн. долларов.

Создание квантового компьютера много лет является целью исследователей по всему миру. Его практическим применением мог бы стать не только взлом шифров, но и, например, поиск новых лекарств или создание искусственного интеллекта.

Гражданские специалисты, работающие над созданием квантового компьютера, давно пытаются оценить, как далеко продвинулись их коллеги из АНБ. Хотя достоверных сведений нет, судя по документам, предоставленным Сноуденом, спецслужба пока не ближе к успеху, чем остальные участники гонки. Кроме того, предполагается, что успех в таком деле трудно было бы держать в тайне.

Напомним, компания D-Wave Systems уже продает квантовые компьютеры. В числе покупателей компьютера, который, используя квантовую механику, позволяет решить задачи, неподдающиеся традиционным методам решения при приемлемых затратах времени, названы Google, NASA и Universities Space Research Association. Следует уточнить, что этот компьютер не подходит для взлома кодов — его способности не позволяют реализовать необходимый алгоритм.