УДК 004.27:004.056.5

ПРИМЕНЕНИЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

канд. тех. наук, доц. И. Б. БУРАЧЁНОК, А. В. ПОПОВ, В. Д. ШУЛЯК
(Полоцкий государственный университет имени Евфросинии Полоцкой, Беларусь)

Аннотация. *Приведены результаты исследований применения квантовых вычислений в сфере информационной безопасности. Рассмотрены алгоритмы, описывающие принцип работы квантового компьютера: алгоритм Гровера, алгоритм Дойча и алгоритм Бернштейна-Вазирани. Проведенный анализ представленных алгоритмов работы квантового компьютера позволил предсказать направления дальнейшего развития квантовых вычислений в сфере информационной безопасности.*

Ключевые слова: *защита данных, информационная безопасность, квантовые вычисления, квантовые технологии, квантовый компьютер, обработка данных.*

Введение. Темпы роста современных технологий приводят к увеличению объёмов разнообразной информации. Современным компьютерам становится с каждым днем сложнее справляться с обработкой большого количества данных в различных сферах деятельности человека, которые необходимы, например: при решении стратегических задач; при криптоанализе; в системах обнаружения вторжений; при обработке сигналов; при расчете траекторий движущихся объектов в воздушном или космическом пространстве и т.п. При поиске решений перечисленных задач посредством современных вычислительных устройств главными проблемами являются низкие производительность обработки данных и мощность вычислений. Поэтому на смену современным компьютерам приходят квантовые, принцип которых основан на использовании для вычислений таких квантово-механических явлений, как суперпозиция и запутывание для преобразования входных данных в выходные [1].

Интерес к квантовым компьютерам значительно возрос, когда Канадская компания D-Wave Systems объявила о продаже первого в мире коммерческого квантового компьютера «Орион» мощностью 16 кубитов [2]. Поэтому **актуальность исследований** в области развития квантовых вычислений в сфере информационной безопасности не вызывает сомнений, так как квантовый компьютер может обеспечить эффективную производительность на 3-4 порядка выше [3], чем любое из современных вычислительных устройств. Однако развитие квантовых технологий

позволяет не только решить задачи, в которых необходимо точное предоставление информации при обработке большого количества данных, но и способствует возникновению новых угроз в сфере информационной безопасности. Уже сегодня можно предположить, что развитие квантовых вычислений позволит формировать кибер-мутации и повлечет за собой эволюцию ландшафта новых киберугроз за счет интеграции квантовых и нейросетевых технологий. Также возникает серьезная угроза и для современных криптографических систем.

Основной **целью представленной работы** является анализ известных квантовых алгоритмов, применение которых в сфере информационной безопасности позволит не только спрогнозировать и предотвратить новые киберугрозы, но и создать современные гибкие и устойчивые системы безопасности и защиты информации.

Если рассматривать современный компьютер, то в качестве минимальной логической единицы он имеет размерность бит (бит может принимать всего два значения – 0 или 1). Квантовый компьютер в отличие от обычного, оперирует квантовыми битами или сокращенно – кубитами. Особенность кубитов в том, что они могут одновременно принимать значения и 0, и 1, и все значения комбинаций этих 2-х составляющих, так как кубиты имеют не материальную (физическую), а квантовую природу. Это позволяет квантовым вычислительным устройствам используя способность кубита принимать одновременно несколько значений (количество состояний (значений) кубита бесконечно) и решать большое количество задач параллельно и одновременно.

Проведенный анализ источников по решению задач в их квантовом представлении позволил выделить перечень квантовых алгоритмов, которые можно классифицировать в соответствии с их отличительными особенностями [2]:

– алгебраические и теоретико-числовые алгоритмы, которые представляют из себя методы решения задач, связанные с факторизацией чисел основываясь, к примеру, на теории чисел, теории групп, теории графов, теории числовых полей, а также на теории эллиптических кривых и др.;

– оракульные алгоритмы, основывающиеся на понятии чёрного ящика и которые могут выполнять разного рода операции над входными данными;

– алгоритмы аппроксимации и моделирования, использующиеся для нахождения приблизительного решения сложно смоделированных задач;

– алгоритмы оптимизации и машинного обучения, основанные на методах, позволяющих быстрее адаптироваться под количество найденных решений.

Квантовые алгоритмы можно также классифицировать по типу квантовых преобразований. Среди часто используемых преобразований можно отметить:

– фазовый откат [1], являющийся распространенным и полезным методом решения задач черного ящика в квантовых вычислениях или решении задач по определению информации о неизвестной функции;

– фазовую оценку, позволяющую использовать правильно преобразованную информацию для измерения и интерпретации ее в классическом представлении;

– квантовые преобразования Фурье [3], описывающие изменение информации и ее классическое представление, что связывает их с понятием фазовой оценки. Квантовое преобразование Фурье – это вариант дискретного преобразования Фурье, областью значения которого являются равномерно распределенные на интервале $[0,2\pi]$ точки для некоторого N;

– квантовое блуждание – алгоритм, который описывает перемещение значения с помощью представленных ему установок. Для специалистов в IT-сфере или в математике, квантовое блуждание – это, прежде всего, аналог классического блуждания, где вместо преобразования вероятности посредством стохастической матрицы, производятся преобразования амплитуды вероятностей [1].

Квантовое случайное блуждание применяется в двух типах алгоритмов. Первый тип алгоритмов по сравнению с классическими аналогами ориентирован на уменьшение временных затрат. Задача сводится к реализации блуждания по некоторому графу с целью достичь определенной вершины, за минимальное время. Вторая группа алгоритмов предназначена для решения задач поиска. Задача сводится к тому, что необходимо найти вершину графа, наделенную определенным свойством. Такие алгоритмы превосходят классические аналоги по числу шагов: квантовых «шагов» требуется меньше, а значит и работа алгоритма эффективнее;

– усиление амплитуды [1] – представляет собой метод квантовых вычислений, обобщающий идею поискового алгоритма Гровера.

Далее рассмотрим алгоритмы, описывающие принцип работы квантового компьютера. Из самых известных алгоритмов его работы можно выделить алгоритм Гровера, алгоритм Дойча и алгоритм Бернштейна – Вазирани.

Представленные алгоритмы чаще похожи друг на друга тем, что использование квантовых вычислений в них построено на более широком использовании *P* и *NP* сложностей задач по времени [1]. Например, *P* – задачи данного класса решаются с помощью детерминированной машины Тьюринга за полиномиальное время [4]. *NP* – задачи данного класса решаются с помощью недетерминированной машины Тьюринга за полиномиальное время [4]. Понятие *P* классов задач основывается на таких примерах как: существование пути в графе, задача о взаимно простых числах на основе их решения за полиномиальное время. А вот понятие *NP* классов подразумевает собой проверку соответствия за полиномиальное время, а примером таких задач является: задача о клике, задача о выполнимости булевой формулы.

Приведённые выше задачи можно интегрировать с помощью одного из основных квантовых алгоритмов – алгоритма Гровера [2], который представляет из себя решение задач по поиску элементов в неупорядоченном списке и позволяет найти элемент за $0(sqrt(N))$, (где *sqrt* – нахождение арифметического корня

квадратного от числа *N*, а *N* – количество битов в числе) [4]. Поисковый алгоритм Гровера является квантовым алгоритмом, который способен решить задачу полного перебора, т.е. получить вывод уравнения $f(x)=1$, при котором *f* есть функция *n* переменных.

Алгоритм Дойча работает иначе. Он напоминает понятие *NP*-сложности. Алгоритм построен таким образом, что он решает задачу проверки корректности функции и состоит из нескольких этапов, таких как: подготовка квантового состояния (этап происходит за счёт различных операций, присущих квантовому компьютеру), а дальше идёт сама проверка корректности функции (для этого используются так называемые квантовые вентили, которые позволяют выполнить эту проверку), последним этапом является извлечение результата с помощью измерения квантового состояния.

Чтобы найти определённое число при вычислении скалярного произведения с некоторым неизвестным *n*-битным числом *a* по модулю 2 в классическом представлении вычислений понадобится несколько обращений к функции, а алгоритм Бернштейна-Вазирани осуществляет это же за одно обращение. Сама работа алгоритма организовывается на получение равномерной суперпозиции всех возможных входов для функций [3].

Это далеко не весь перечень современных квантовых алгоритмов. К этому перечню можно добавить: алгоритм Дойча-Джозса, алгоритм Залки-Вигнера, алгоритм Саймона, адиабатические квантовые алгоритмы, алгоритмы факторизации Шора, квантовые алгоритмы контролируемого/неконтролируемого машинного обучения, алгоритмы квантового хеширования, алгоритмы обучения квантовой нейронной сети на основе принципа суперпозиции.

Проведенные исследования известных методов функционирования квантовых алгоритмов и возможностей их применения в сфере информационной безопасности позволяют решить проблемы конфиденциальности и контроля данных еще на этапе развития квантовых компьютеров и алгоритмов их работы.

Вывод. Несмотря на то, что на сегодня промышленных образцов квантового компьютера в природе пока еще не существует и к настоящему времени формируются лишь принципы его работы, а появление реально действующих устройств зависит от прогресса высоких технологий, в том числе нанотехнологий, имеющих дело с микродеталями размером порядка длины световой волны или даже меньше, а также с прогрессом нанофотоники, а в лабораторных условиях созданы лишь прототипы логических квантовых ячеек, специалистам в области информационной безопасности приходится быть в боевой готовности и, исследуя реальные и потенциальные сценарии будущего, готовить новые линии обороны и защиты информации.

Согласно проведенного анализа стремительный рост квантовых вычислений и их внедрение в информационные технологии, а также возможности представленных алгоритмов и их преобразований позволят значительно улучшить решение следующих специфических задач:

- проведение кибербразведки,
- обнаружение и реагирование на киберугрозы,
- анализ уязвимостей и управление ими,
- обеспечение безопасности конечных точек,
- управление идентификацией и доступам к системам безопасности и пр.

Однако для обеспечения информационной безопасности в эпоху квантовых вычислений можно указать и другие наиболее актуальные направления развития:

- необходимо усиливать и усовершенствовать алгоритмы шифрования;
- вводить многофакторную аутентификацию;
- осуществлять процесс минимизации данных;
- проводить постоянное обучение и повышать осведомленность пользователей;
- осуществлять регулярное обновление систем безопасности;
- проводить проверку достоверности хранимых данных;
- внедрять и совершенствовать политику конфиденциальности и согласия;
- на регулярной основе проводить резервное копирование и восстановление хранимых данных;
- осуществлять аудит и оценку уязвимостей;
- организовывать управление доступом и сегментацию.

Перечисленные направления развития в сфере информационной безопасности позволят создать современные гибкие и устойчивые системы безопасности и защиты информации.

ЛИТЕРАТУРА

1. Гузик, В. Ф. Высокопроизводительные вычислительные системы и квантовая обработка информации : учебное пособие : [16+] / В. Ф. Гузик, С. М. Гушанский, Е. В. Ляпунцова, В. С. Потапов ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2021. – 202 с.
2. Гузик, В. Ф. Основы теории построения квантовых компьютеров и моделирование квантовых алгоритмов : монография / В. Ф. Гузик, С. М. Гушанский, Е. В. Ляпунцова, В. С. Потапов. – Москва : Физматлит ; Ростов-на-Дону – Таганрог : Издательство Южного федерального университета, 2019. – 287 с.
3. Гушанский, С. М. Методика разработки и построения квантовых алгоритмов [Текст] / С. М. Гушанский, В. С. Потапов // Информатизация и связь. – 2017. – № 3. – С. 101–104.
4. Котов, В.М. Алгоритмы и структуры данных: учеб. пособие / В. М. Котов, Е. П. Соболевская, А. А. Толстиков. – Минск : БГУ, 2011. – 267 с. – (Классическое университетское издание).