

**Запольская Татьяна Александровна**  
магистрант кафедры «Кибербезопасность информационных систем»  
ФГБОУ ВО «Донской государственной технической университет»  
г. Ростов-на-Дону, Россия  
*Научный руководитель:*

**Сосновский Иван Александрович**  
к.т.н., доцент кафедры «Кибербезопасность информационных систем»  
ФГБОУ ВО «Донской государственной технической университет»  
г. Ростов-на-Дону, Россия

### **Постквантовая криптография в условиях развития квантовых вычислений**

**Аннотация.** Статья посвящена актуальной проблеме обеспечения кибербезопасности в условиях появления квантовых компьютеров, которые представляют угрозу для традиционных криптографических алгоритмов. В качестве решения рассматривается новая технология - постквантовая криптография. В работе подробно раскрывается сущность и принцип действия одного из самых перспективных направлений PQC - криптографии на решётках, основанной на вычислительной сложности задачи о кратчайшем векторе в многомерном пространстве. Статья также освещает практические аспекты внедрения PQC для защиты коммуникаций, цифровых подписей и долгосрочных данных, а также анализирует основные вызовы, связанные с предстоящим глобальным переходом на новые стандарты шифрования.

**Ключевые слова:** кибербезопасность, безопасность информации в сети, информационные системы, базы данных, несанкционированный доступ, постквантовая типология, защита от кражи данных.

**Zapolskaya Tatyana Alexandrovna**  
Master's student of the Department of Cybersecurity of information systems  
Don State Technical University  
Rostov-on-Don, Russia  
*Scientific Supervisor:*

**Sosnovskiy Ivan Alexandrovich**  
Candidate of Technical Sciences,  
Associate Professor of the Department of Cybersecurity of Information Systems  
Don State Technical University  
Rostov-on-Don, Russia

### **Post-quantum cryptography in the context of quantum computing development**

**Abstract.** The article is devoted to the urgent problem of ensuring cybersecurity in the context of the emergence of quantum computers, which pose a threat to traditional cryptographic algorithms. A new technology, post - quantum cryptography, is being considered as a solution. The paper reveals in detail the essence and principle of operation of one of the most promising areas of PQC cryptography on lattices, based on the computational complexity of the problem of the shortest vector in a multidimensional space. The article also highlights the practical aspects of implementing PQC to protect communications, digital signatures, and long-term data, as well as analyzes the main challenges associated with the upcoming global transition to new encryption standards.

**Keywords:** cybersecurity, information security in the network, information systems, databases, unauthorized access, post-quantum printing, data theft protection.

Традиционные методы шифрования на сегодняшний день отходят на второй план, причиной этого является появление квантовых компьютеров, машин, чья вычислительная мощность ставит под угрозу самые сложные из современных криптографических алгоритмов. В кибербезопасности появляется понятие «постквантовая криптография». Это не просто обновление старых протоколов, а принципиально новый подход к созданию цифровой безопасности.

Большинство современных систем шифрования основаны на сложности решения определенных математических задач - разложения больших чисел на множители или дискретного логарифмирования. Для классического компьютера эти задачи требуют большого количества времени. Однако алгоритмы, запущенные на достаточно мощном квантовом компьютере, решают их с большой эффективностью, делая существующую защиту бесполезной.[1]

Постквантовая криптография (Post-Quantum Cryptography (далее PQR)) - это не один алгоритм, а совокупность криптографических алгоритмов, которые устойчивы к атакам как с использованием классических, так и квантовых компьютеров. Их принципиальное отличие заключается в том, что в основе лежат математические задачи, которые остаются сложными даже для квантового процессора. Вместо факторизации чисел PQC использует другие, более устойчивые к нападениям злоумышленников разделы математики.

Наиболее перспективным и универсальным считается направление криптографии на решётках. Разберем его подробно далее, так как именно оно, с высокой вероятностью, ляжет в основу цифровой безопасности.[2]

В математике решётка - это не периодическая структура, как в кристалле, а бесконечный набор точек в многомерном пространстве, упорядоченных с определенным шагом. Принцип безопасности заключается в следующем. Сложность, на которой строится безопасность, называется «задачей о кратчайшем векторе». Если дана многомерная решётка с тысячами измерений, необходимо найти в ней самую короткую линию, соединяющую две точки (самый короткий вектор). Для классического и для квантового компьютера эта задача является вычислительно неразрешимой при достаточно больших размерах решётки. Можно легко сгенерировать решётку с ключом (базисом), который позволяет легко ориентироваться в ней и решать задачу, но для внешнего наблюдателя без этого ключа поиск кратчайшего вектора осложнен, так как ключ находится в 1000-мерном пространстве.

К ключевым преимуществам технологии относятся:

1. Стойкость к квантовым атакам: на сегодняшний день не известно алгоритмов, которые бы эффективно взламывали хорошо подобранные решёточные системы на квантовом компьютере;

2. Гибкость и универсальность: на основе решёток можно построить все необходимые криптографические примитивы: асимметричное шифрование (для обмена ключами), цифровые подписи (для аутентификации);

3. Высокая производительность: алгоритмы на решётках, как правило, работают быстрее и требуют меньше вычислительных ресурсов, чем некоторые их конкуренты, что критически важно для высоконагруженных систем.

4. Внедрение PQC - это не просто замена одного алгоритма на другой. Это масштабная миграция всей цифровой экосистемы.

Защищенные коммуникации: браузеры, мессенджеры и VPN-сервисы будут использовать PQC-алгоритмы для установления безопасного соединения. Это гарантирует то, что перехваченное сегодня зашифрованное сообщение нельзя будет расшифровать завтра, когда квантовые компьютеры станут мощнее.[3]

Юридически значимые документы, программное обеспечение и транзакции в блокчейне будут подписываться PQC-подписями. Это защитит их от подделки в будущем. Это технологии цифровой подписи на сегодняшний день.

Информация, которая должна храниться долгое время в архивах, тоже должна быть защищена. К таким архивным данным относятся государственные архивы, медицинские карты, коммерческие секреты. Уже сегодня такие данные должны шифроваться с использованием PQC, иначе они станут уязвимыми задолго до истечения своего срока конфиденциальности.

Переход на постквантовую криптографию - сложнейшая задача. Основные вызовы включают:

1. Стандартизация – проведение конкурса на отбор лучших PQC-алгоритмов;
2. Совместимость – внедрение новых алгоритмы в миллиарды устройств по всему миру, от мощных серверов до крошечных IoT-датчиков;
3. Криптографическая гибкость: эксперты рекомендуют стратегию "квантовой миграции", когда системы используют и классические, и PQC-алгоритмы одновременно, создавая многоуровневую защиту.[4]

Таким образом, постквантовая криптография - это стратегический и необходимый ответ на экзистенциальную угрозу квантовых вычислений. Она представляет собой переход от эпохи, когда наша безопасность основывалась на вычислительных ограничениях, к эпохе, где она будет базироваться на непреодолимой математической сложности.

Инвестируя и внедряя PQC сегодня, мы строим не просто защиту от угрозы будущего; мы закладываем фундамент цифрового доверия, который будет оберегать частную жизнь, финансовые активы и национальную безопасность на десятилетия вперед.

#### **Список источников**

1. Национальный институт стандартов и технологий (NIST). Post-Quantum Cryptography Standardization. <https://csrc.nist.gov/projects/post-quantum-cryptography> (дата обращения 02.11.2025г.);
2. Александра Болдырева, Михаил Бородин. «Постквантовая криптография: начало пути». «Открытые системы. СУБД». Журнал. - № 03, 2020. С.28-69;
3. Пейкерт, К. (2016). Десятилетие решетчатой криптографии. Основы и тенденции в теоретической информатике, том 10, № 4, С. 283-424;
4. Моска, М. (2018). Кибербезопасность в эпоху квантовых компьютеров: будем ли мы готовы? IEEE Security & Privacy, том 16, № 5, С. 38-41.