квУДК 004

Четин А.О.

магистр

Научный руководитель: Волков К.А., к.т.н.

Поволжский государственный университет телекоммуникаций и информатики

ПОТЕНЦИАЛЬНЫЕ ВОЗМОЖНОСТИ ВНЕДРЕНИЯ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА СЕТЯХ СВЯЗИ

Аннотация: в работе рассматриваются потенциальные возможности внедрения систем квантового распределения ключа в волоконно-оптических линиях связи. Представлен аналитический обзор современных систем квантового распределения ключа на сетях связи, представлены достоинства и недостатки данной технологии.

Ключевые слова: квантовое распределение ключей, волоконно-оптические линии связи.

Chetin A.O.

master's degree

Scientific supervisor: Volkov K.A., Ph.D.

Povolzhskiy State University of Telecommunications and Informatics

POTENTIAL POSSIBILITIES OF IMPLEMENTING QUANTUM KEY DISTRIBUTION SYSTEMS ON NETWORKS

***Abstract**: the paper examines the potential for implementing quantum key distribution systems in fiber-optic communication lines. An analytical review of modern quantum key distribution systems in communication networks is presented, and the advantages and disadvantages of this technology are presented.*

***Keywords**: quantum key distribution, fiber optic communication lines.*

Квантовое распределение ключей (КРК) в оптических линиях - это технология, использующая принципы квантовой механики для безопасной передачи криптографических ключей. В отличие от классических методов

шифрования, безопасность КРК основана на законах физики, а не на вычислительной сложности алгоритмов [1-5].

Как известно, КРК использует квантовые состояния света для передачи информации. Любая попытка перехвата или измерения этих состояний неизбежно вносит изменения, которые могут быть обнаружены легитимными участниками обмена. Для обмена сообщениями используются различные протоколы КРК, такие как BB84, E91 и другие. Они отличаются способами кодирования и передачи квантовых состояний [5].

КРК обычно реализуется с использованием оптических волокон, так как они обеспечивают относительно низкие потери при передаче оптического излучения.

Ключевое преимущество КРК - его теоретическая безопасность. Любая попытка прослушивания канала связи неизбежно приводит к внесению ошибок, которые могут быть обнаружены. Но при этом КРК имеет ограничения, такие как расстояние передачи (из-за потерь в оптическом волокне), необходимость в специализированном оборудовании и чувствительность к шумам и помехам [1-2].

В целом, КРК представляет собой перспективную технологию для обеспечения безопасной связи, особенно в ситуациях, где требуется максимальная защита от перехвата информации.

КРК позволяет обнаруживать любые попытки перехвата или прослушивания канала связи. Любая попытка измерить квантовые состояния, используемые для передачи ключа, вносит изменения, которые могут быть обнаружены легитимными участниками обмена. Это позволяет им прервать передачу ключа и избежать компрометации.

КРК обеспечивает защиту от будущих угроз, таких как появление квантовых компьютеров, которые могут взломать существующие криптографические алгоритмы. КРК не зависит от вычислительной сложности и поэтому остается безопасным даже при наличии квантовых компьютеров [5].

Безопасность КРК не зависит от каких-либо математических предположений или гипотез, которые могут быть опровергнуты в будущем. Это делает КРК более надежным и устойчивым к новым атакам и обеспечивает долгосрочную безопасность, поскольку его безопасность не ухудшается со временем (в отличие от классических методов, которые могут стать уязвимыми с развитием технологий). И конечно же, такой подход дает возможность интеграции с существующими системами шифрования для повышения их безопасности. Квантовый ключ может быть использован для шифрования данных с помощью классических алгоритмов шифрования.

Несмотря на эти преимущества, стоит отметить, что КРК также имеет некоторые ограничения, такие как расстояние передачи, стоимость оборудования и чувствительность к шумам. Однако, развитие технологий КРК направлено на преодоление этих ограничений и расширение области применения. Хотя КРК предлагает значительные преимущества в области безопасности, она также имеет ряд недостатков, которые необходимо учитывать. Одним из основных ограничений КРК является расстояние, на которое можно безопасно передавать ключи. На больших расстояниях требуется использование квантовых повторителей, которые являются сложными и дорогими устройствами. Оборудование для КРК, такое как источники одиночных фотонов, детекторы и системы управления, является сложным и дорогим. Это делает КРК менее доступным для широкого применения [5].

Также скорость генерации и передачи ключей в КРК обычно ниже, чем в классических системах распределения ключей. Это может быть проблемой для приложений, требующих высокой пропускной способности. Для реализации КРК требуется специальная инфраструктура, включая квантовые каналы связи и доверенные узлы. Это может быть сложно и дорого реализовать, особенно в существующих сетях связи.

Уязвимости в реализации: Хотя теоретически КРК является безопасным, на практике его безопасность может быть скомпрометирована

из-за уязвимостей в реализации оборудования и программного обеспечения. Например, несовершенство детекторов может быть использовано для проведения атак. Безопасность КРК зависит от надежности и честности производителей оборудования. Если в оборудовании есть скрытые дефекты или "закладки", это может поставить под угрозу безопасность системы [1].

Отсутствие стандартов: В настоящее время не существует общепринятых стандартов для КРК, что затрудняет совместимость между различными системами и усложняет внедрение КРК в широком масштабе.

Экономический эффект от применения квантовых систем передачи ключей - сложный вопрос, так как технология находится на относительно ранней стадии развития и широкого распространения еще не получила. Однако, можно выделить несколько ключевых аспектов, которые формируют экономический эффект.

Защита от утечек данных: КРК обеспечивает более высокий уровень защиты от перехвата и расшифровки конфиденциальной информации, что снижает риск утечек данных, которые могут привести к значительным финансовым потерям (штрафы, судебные издержки, компенсации клиентам).

Компании, использующие КРК, могут демонстрировать своим клиентам приверженность к безопасности данных, что может повысить доверие и лояльность клиентов.

Использование передовых технологий, таких как КРК, может привлечь инвестиции и улучшить имидж компании и, конечно же, выход на новые рынки: КРК может позволить компаниям выйти на новые рынки, где требуется высокий уровень безопасности данных (например, в оборонной промышленности или в сфере финансовых услуг).

Развитие и внедрение КРК стимулирует инновации в области квантовых технологий и криптографии, что может привести к созданию новых продуктов и услуг. Развитие рынка КРК создает новые рабочие места для специалистов в области квантовых технологий, криптографии и информационной безопасности.

КРК может использоваться для защиты государственных секретов и конфиденциальной информации от иностранных разведок. Обеспечение безопасной связи: КРК может использоваться для обеспечения безопасной связи между правительственными учреждениями и военными подразделениями.

В заключение, экономический эффект от применения КРК является потенциально значительным, но требует дальнейших исследований и разработок для снижения стоимости и повышения эффективности технологии. Квантовые системы передачи ключей пока находятся на стадии внедрения, но уже сейчас некоторые отрасли проявляют к ним значительный интерес и начинают использовать их в пилотных проектах или для защиты наиболее критичных данных. По мере развития технологий и снижения стоимости КРК, ожидается, что их применение будет расширяться и охватывать все больше отраслей.

Использованные источники:

1. Жиляев, А.Е. Сети квантового распределения ключей в кибербезопасности [Текст]: Научное издание / А.Е. Жиляев, А.Г. Сабанов, А.А. Шелупанов, А.А. Конев, Д.С. Брагин; – М: Горячая линия – Телеком, 2023. – 152 с.

2. Ширяев Д. С., Кундиус А. А., Разживина К. Р., Беляков Н. А., Полухин И. С., Колодезный Е. С. Оптическая система для рассылки квантовых ключей по атмосферному каналу связи // Фотон-экспресс. 2023. №6 (190). URL: https://cyberleninka.ru/article/n/opticheskaya-sistema-dlya-rassylki-kvantovyh-klyuchey-po-atmosfernomu-kanalu-svyazi (дата обращения: 10.06.2025).

3. Жиляев, А.Е. Классификация схем выработки и распределения ключей в сетях квантового распределения ключей произвольной топологии // Доклады ТУСУР. 2021. №4. URL: https://cyberleninka.ru/article/n/klassifikatsiya-shem-vyrabotki-i-raspredeleniya-klyuchey-v-setyah-kvantovogo-raspredeleniya-klyuchey-proizvolnoy-topologii (дата обращения: 10.06.2025).

4. Лойко В.И., Хисамов Ф.Г., Бобылев М.В. Системы квантового распределения ключа и проблемы их практической реализации // Научный

журнал КубГАУ. 2015. №114. URL: https://cyberleninka.ru/article/n/sistemy-kvantovogo-raspredeleniya-klyucha-i-problemy-ih-prakticheskoy-realizatsii (дата обращения: 09.06.2025).
5. Данеев О. В. О проблеме квантового распределения ключей: состояние и перспективы // Хроноэкономика. 2020. №2 (23). URL: https://cyberleninka.ru/article/n/o-probleme-kvantovogo-raspredeleniya-klyuchey-sostoyanie-i-perspektivy (дата обращения: 10.06.2025).