Список использованных источников
1.Лукашов А. А., Фаерман В. А. Обзор и моделирование типовых аппаратных архитектур систем квантового распределения ключей // Известия Томского политехнического университета. Промышленная Кибернетика. 2025. № 2(3). С. 8–23. DOI:10.18799/29495407/2025/2/89.
2.Трещев И.А., Монастырная Е. И. Событийная формальная модель поведения злоумышленника // Ученые записки КнАГТУ. 2024. № 1(73). С. 42–46.
3.Овсянников А. П., Шабанов Б. М. О проекте межуниверситетской квантовой сети // Программные продукты и системы. 2023. № 4(36). С. 695–702.

Обласов Андрей Александрович, к.э.н., доцент, и. о. зав. каф. «Информационная безопасность автоматизированных систем», oblasov_andrei@mail.ru.
Воропаев Даниил Валерьевич, студ. каф. «Информационная безопасность автоматизированных систем», danvoron481@gmail.com.

УДК 004.056.55

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ: ПЕРСПЕКТИВНАЯ ТЕХНОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Обласов, Д.В. Воропаев
ФГБОУВО «Комсомольский-на-Амуре государственный университет», г. Комсомольск-на-Амуре

Ключевые слова: квантовая криптография, квантовые коммуникации, квантовое распределение ключей, квантовые каналы связи.

Современный мир стремительно развивается благодаря информационным технологиям, а объём цифровых данных растет с каждым днем. Традиционные методы шифрования начинают терять свою надёжность в свете возможного появления квантовых компьютеров, способных быстро взломать современные криптографические алгоритмы. В такой ситуации особое значение приобретает технология квантового распределения ключей обеспечивающие невозможность несанкционированного перехвата и доступа [1].

Технология квантового распределения ключей (Quantum Key Distribution - QKD) предназначена для безопасной передачи симметричных ключей шифрования между двумя сторонами. Основываясь на законах квантовой механики, она использует свойства квантовых состояний: любые попытки наблюдения или копирования квантовых состояний неизбежно вызывают их изменения, что позволяет обнаружить факт возможной атаки в режиме реального времени [1].

Основные принципы QKD.

1. Невозможно одновременно точно измерить две взаимно дополняющие характеристики частицы (например, импульс и координату), что предотвращает точное считывание квантового состояния посторонними лицами (принцип неопределенности Гейзенберга);

2. Запрещение клонирования неизвестных квантовых состояний [2]: согласно теореме Нельсона—Уолтера, нельзя идеально скопировать произвольное неизвестное квантовое состояние, что дополнительно усложняет атаку на квантовый канал.

3. Использование квантовых свойств световых частиц [2] (фотонов): фотоны используются для передачи бинарных значений путем манипуляции их поляризацией или фазой, что обеспечивает надежную передачу зашифрованных данных.

Наиболее известными протоколами квантового распределения ключей являются:

а) BB84: первый широко используемый протокол, разработанный Беннеттом и Брассардом в 1984 году [3]. Основой протокола служит четырёхпозиционное представление двух ортогональных базисов, позволяющее обнаружить нарушения безопасности;

б) B92 является упрощённым вариантом BB84, его предложил Чарльз Беннетт в 1992 году (используется два ортогональных состояния, уменьшая сложность оборудования) [3];

в) Ekert91 протокол, основанный на принципе запутанности квантовых состояний, позволяющий добиться большей степени защищённости предложил Артур Эккерт в 1991 году [3].

Этапы передачи ключа в рамках QKD.

1. Генерация фотонов. Источник излучения создаёт поток одиночных фотонов, каждый из которых несет один бит информации, закодированный в поляризации или фазе.

2. Передача и приём. Передающая сторона отправляет последовательность фотонов принимающей стороне, которая производит замеры их состояния с помощью специализированного детектора.

3. Коррекция ошибок. Обе стороны сверяют случайно выбранные части полученного ключа, чтобы убедиться в отсутствии ошибок и возможности атаки.

4. Формирование финального ключа. Остальная часть ключа используется для последующей передачи информации с применением стандартных методов шифрования.

В области технологии QKD для обеспечения дальней связи в развернутых сетях передачи данных проводились испытания коммерческой группой из Германии [4]. В ходе испытания использовался двухполосный протокол QKD через сеть в 254 км, без использования криогенного охлаждения со скоростью распределения ключей в 110 бит/с [4]. Испытания показали возможность внедрения технологии в

масштабируемые сети, в том числе в существующую телекоммуникационную сеть.

Технология QKD находит своё применение в различных сферах. В первую очередь там, где важна высокая степень защиты информации. Например, банковский сектор, используя QKD для передачи финансовой информации гарантирует безопасность транзакций и предотвращение мошенничества, государственные органы применяя технологию квантового распределения ключей повышают защищённость передачи конфиденциальных данных, в телекоммуникации организуются защищённые линий связи, исключающие возможность несанкционированного прослушивания. Концепция квантового распределения ключей открывает новые горизонты в области информационной безопасности, предлагая надежный механизм защиты данных, не зависящий от вычислительных мощностей противника.

Список использованных источников

1.Zapatero V., Zhang Q., Weinfurter H. Advances in device-independent quantum key distribution //npj Quantum Inf. 2023. Vol. 9(10). pp. 105-117. DOI:10.1038/s41534-023-00684-x.

2.Колыхалов Г.А., Кравченко Е.Г. Интерпретация квантов энергии и массы фотона с позиций закона всемирного тяготения //Учёные записки КнАГТУ. 2025. №7(87). С. 109 – 114.

3.Кунуспаев Д.С., Шойынбек А. Роль квантовой криптографии в развитии цифровой экономики: исследование стойкости протоколов распределения ключей // Вестник науки. 2026. №2(95) том 1. С. 745 – 769.

5.Pittuluga M., Brzosko A., Long-distance coherent quantum communications in deployed telecom networks // Nature. 2025. Vol. 640. pp. 911-917. DOI:10.1038/s41586-025-08801-w.

Обласов Андрей Александрович, к.э.н., доцент, и. о. зав. каф. «Информационная безопасность автоматизированных систем», oblasov_andrei@mail.ru.
Воропаев Даниил Валерьевич, студ. каф. «Информационная безопасность автоматизированных систем», danvoron481@gmail.com.

УДК 519.7; 004.2; 004.3

О ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВАХ, ИСПОЛЬЗУЮЩИХ СХЕМУ QAM-OFDM МОДУЛЯЦИИ

В.П. Цветов
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: гибридные детерминированно-стохастические вычислительные системы, радио биты.