Проведённые эксперименты подтвердили высокую эффективность предложенного метода. Модель HADFM достигла значения Macro F1-score 0,9952 при классификации уровней риска, а модель Deep SVDD обеспечила Recall 98,7% при обнаружении аномалий. Совместное применение моделей обеспечивает точность выявления потенциально опасных действий пользователей на уровне 99,2%.

Полученные результаты подтверждают эффективность применения многофакторного анализа комбинаций поведенческих признаков в задачах выявления утечек данных и демонстрируют перспективность использования предложенного подхода при разработке интеллектуальных модулей UEBA и DLP-систем.

Список использованных источников

1.Owobu, W.O. Conceptual Framework for Deploying Data Loss Prevention and Cloud Access Controls in Multi-Layered Security Environments / W.O. Owobu, O.A. Abieba, P. Gbenle [et al] // International Journal of Multidisciplinary Research and Growth Evaluation. – 2022. – Vol. 3(1). – P. 850-860.

2.Савенков, П.А. Использование методов и алгоритмов анализа данных и машинного обучения в UEBA/DSS для поддержки принятия управленческих решений / П.А. Савенков, П.С. Трегубов // Моделирова-ние, оптимизация и информационные технологии. – 2020. – Т. 8(1). – С. 585-587.

3.Ruff, L. Deep One-Class Classification / L. Ruff, R.A. Vandermeulen, N. Gornitz [et al.] // Proceedings of the 35th International Conference on Machine Learning (ICML). – 2018. – P. 4393-4402.

Марченко Екатерина Александровна, студ. гр. 6133-010402D, ea_marchenko_dev@mail.ru.
Жуков Семён Викторович, старш. препод. каф. геоинформатики и информационной безопасности, svzhukov@ssau.ru.
Федосеев Виктор Андреевич, к.физ.-мат.наук, доцент, зав. каф. геоинформатики и информационной безопасности, fedoseev.va@ssau.ru.

УДК 004.056.5; 004.7

КВАНТОВО-ЗАЩИЩЁННЫЕ СЕТИ: ПЕРСПЕКТИВЫ РАЗВИТИЯ И ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ

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

Ключевые слова: квантово-защищённые сети, квантовые коммуникации, характеристики квантовых сетей.

Квантово-защищённые сети представляют сложную структуру, включающую несколько ключевых компонентов, каждый из которых играет важную роль в обеспечении надежной и безопасной передачи данных.

Источником одиночных фотонов является устройство, генерирующее отдельные фотоны света, которые передают информацию о ключе шифрования.

Выделяют три основных типа генераторов одиночных фотонов [1]:

а) светодиоды (простые и недорогие устройства, испускающие фотоны при подаче электрического тока);

б) лазеры (гарантируют стабильность и высокое качество фотонного потока, но стоят дороже и сложнее в эксплуатации и параметрическое преобразование (метод, основанный на нелинейных кристаллах, генерирующий пары запутанных фотонов, улучшающий безопасность передачи);

в) детекторы предназначены для регистрации отдельных фотонов, полученных от источника. От чувствительности и точности детекторов зависят надёжность и скорость передачи данных. В качестве основных типов детекторов выделяют лавинный фотодиод одиночных фотонов, сверхпроводящий нанопроволочный детектор одиночных фотонов и переохлажденные детекторы.

Контроллеры синхронизации отвечают за согласованную работу всех узлов квантово-защищённой сети. Они управляют процессом передачи и приема данных, осуществляют коррекцию ошибок и обработку результатов измерений.

Интерфейсы подключения позволяют интегрировать квантово-защищённую сеть в обычные компьютерные сети. Обычно это реализуется через Ethernet-порт или специальный модуль, соединяющий квантовый канал с сервером или рабочей станцией. Важнейшим требованием к интерфейсам является низкая задержка и минимальные потери пакетов.

Помимо квантового канала, квантово-защищённые сети используют традиционный канал связи для координации действий участников. Поскольку классический канал доступен злоумышленникам [2], он нуждается в дополнительной защите. Здесь применяются криптографические методы и контроль целостности сообщений, обеспечивая надёжность передачи служебной информации.

Дополнительные компоненты квантово-защищённых сетей состоят из усилителей и повторителей сигнала (расширение зоны покрытия), элементов системы мониторинга и диагностики (контроль работоспособности сети, аппаратуры резервирования и аварийного восстановления (обеспечение непрерывности передачи данных).

В ходе экспериментов были выявлены следующие функциональные возможности и качественные показатели квантово-защищённых каналов:

1) средняя скорость передачи составляет около 1 мегабита в секунду на коротких дистанциях (менее 1 км) [1];

2) средняя скорость передачи составляет около нескольких десятков килобит в секунду на расстояниях порядка 100 км [1];

3) уровень ошибок при правильной настройке оборудования колеблется в пределах 1% [1].

Данные показатели приемлемы для решения большинства реальных задач и тесты подтвердили невозможность скрытого перехвата информации без разрушения квантового состояния фотонов, подтверждающего факт нарушения.

Натурные испытания продемонстрировали способность квантово-защищённых каналов надежно функционировать в реальных условиях городской и пригородной среды.

Тестирования проводились в условиях плотной застройки городов Москвы и Санкт-Петербурга [3], подтвердив работоспособность технологии даже при наличии большого количества помех и препятствий, удалось установить квантово-защищённое соединение на расстояние свыше 100 км, подтвердив возможность коммерческого использования технологии для межгородских связей [3]. Данное испытание показало возможность интегрирования в существующую телекоммуникационную инфраструктуру без существенных изменений.

Необходимо отметить, что в ходе испытаний также были выявлены некоторые проблемы и ограничения. Массовое внедрение технологии требует дорогостоящего оборудования, необходим постоянный низкотемпературный режим и отсутствие вибраций [3]. Кроме того, процедура установления надежного соединения занимает значительное время, что снижает общую пропускную способность системы [3].

Испытания квантово-защищённых сетей активно проводятся учёными многих государств. В Европе (в городских условиях), Японии (в условиях в условиях тесно контролируемого испытания), Китае (испытания при протяженности сети длиной более 2 тыс. км.), США (в условиях загруженной сети), в Бразилии (в ограниченных условиях с оценкой эксплуатационных показателей), Аргентине (с акцентом на разработку методов коррекции ошибок), в ОАЭ (в условиях жаркого климата) и Египте (с акцентом на банковский сектор) проводились испытания, для решения проблемы создания надёжных квантово-защищённых сетей.

Международные исследования демонстрируют успешные эксперименты по квантово-защищённым каналам связи в разных странах, включая крупные города и сложные условия эксплуатации. Результаты подтверждают перспективность квантовой криптографии для практического применения и повышения уровня информационной безопасности в цифровую эпоху.

Выявленные ограничения и особенности указывают направление для дальнейших исследований и разработок, целью которых должно стать устранение недостатков и повышение удобства использования квантовых технологий.

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.