Приложение № 4
к образовательной программе среднего профессионального образования – программе подготовки специалистов среднего звена по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (на базе основного общего образования)

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «НАУЧНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «СИРИУС»
(АНОО ВО «УНИВЕРСИТЕТ «СИРИУС»)

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«Квантовые коммуникации и квантовая криптография»

1. Трудоемкость профессионального модуля: 306 ак.ч.

2. Место профессионального модуля в учебном плане:

Профессиональный модуль «Квантовые коммуникации и квантовая криптография» входит в образовательный компонент программы П.00 «Профессиональный цикл» (ПМ.08) и является вариативным. Профессиональный модуль реализуется в 5-6 семестрах.

3. Цель профессионального модуля: формировать у обучающихся профессиональные компетенции для применения принципов квантовых коммуникаций и квантовой криптографии в целях обеспечения высокого уровня защиты информации в информационно-телекоммуникационных системах, включая понимание фундаментальных основ и практическое освоение соответствующих технологий.

4. Задачи профессионального модуля:

– изучить теоретические основы квантовых коммуникаций и квантовой криптографии: освоить ключевые принципы квантовой физики, лежащие в основе технологий защиты информации (принцип неопределённости Гейзенберга, квантовая запутанность, теорема о запрете клонирования); базовые протоколы квантового распределения ключей (например, BB84, E91); преимущества квантовой криптографии перед классическими методами шифрования;

– ознакомиться с архитектурой и компонентами систем квантовых коммуникаций: изучить типы квантовых каналов связи (оптоволоконные, атмосферные, спутниковые), оборудование для генерации и детектирования одиночных фотонов, устройства квантового распределения ключей (QKD-системы); проанализировать существующие решения и стандарты в области квантовых коммуникаций, а также оценить их применимость в реальных информационно-телекоммуникационных инфраструктурах;

– освоить методы развёртывания и эксплуатации систем квантовой криптографии: научиться настраивать и интегрировать QKD-устройства в существующие сети; отработать процедуры генерации, распределения и управления квантовыми ключами; изучить способы сопряжения квантовых систем с традиционными средствами шифрования и инфраструктурой открытых ключей (PKI); приобрести навыки мониторинга и диагностики работоспособности квантовых каналов;

– развить навыки оценки эффективности и безопасности квантовых решений для защиты информации: научиться анализировать устойчивость квантовых протоколов к потенциальным атакам; освоить методы расчёта дальности и скорости передачи квантовых ключей в зависимости от параметров канала; изучить нормативные требования и ограничения к внедрению квантовых технологий; оценить экономические и технические перспективы масштабирования квантовых коммуникаций в корпоративных и государственных сетях.

5. Перечень разделов (тем) профессионального модуля и их краткое содержание:

Наименования разделов (тем) профессионального модуля	Содержание разделов (тем) профессионального модуля
МДК.08.01 Квантовые коммуникации	

Тема 1. Введение в квантовую криптографию	Понятие квантовой криптографии. Место в системе современных методов защиты информации. Проблема распределения ключей в классической криптографии. Угроза квантовых вычислений для асимметричных криптосистем (алгоритм Шора).
Тема 2. Основные понятия квантовой механики для ИБ	Кубит. Принципы суперпозиции и запутанности. Состояния
Тема 3. Квантовые генераторы случайных чисел (QRNG)	Проблема истинной случайности. Отличие квантовых генераторов от классических (детерминированных). Схемы QRNG: на основе фазовых флуктуаций, оптических ответвлений, расщепления фотонов. Применение в криптографии.
Тема 4. Физическая реализация квантовых коммуникаций	Одиночные фотоны как носители информации. Источники фотонов (ослабленный лазер, параметрическое преобразование). Детекторы фотонов (лавинные фотодиоды). Оптоволоконные и свободно-пространственные линии связи. Проблема потерь и деполяризации.
Тема 5. Основные протоколы квантового распределения ключей (QKD)	Протокол BB84 (Беннетт — Брассар, 1984): поляризационное и фазовое кодирование. Согласование базисов. Оценка квантовой битовой ошибки (QBER). Приватность усиления. Протокол E91 (Экерт, 1991) — использование запутанных состояний. Протокол B92.
Тема 6. Анализ безопасности QKD	Информационная безопасность QKD. Теоретические основы: теорема о невозможности клонирования. Атаки: «перехват-ретрансляция» (intercept-resend), атака с разделением по числу фотонов (PNS), атака с ослеплением детектора. Методы противодействия.
МДК.08.02 Квантовая криптография	
Тема 1. Программно-аппаратные комплексы QKD	Обзор существующих коммерческих систем QKD (ID Quantique, Toshiba, QRate, «Кулон»). Архитектура QKD-устройства: передающая и приемная части, постобработка, интерфейсы для СЗИ. Стандартизация QKD (ETSI, ISO, ТК 26 РФ).
Тема 2. Квантовые сети и доверенные узлы	Понятие квантовой сети. Топологии: точка-точка, звезда, кольцо. Доверенные узлы и их роль. Квантовые повторители. Управление ключами в сети (KMS — Key Management System).
Тема 3. Интеграция QKD в существующие сети связи	Разделение спектра (WDM): квантовый и классический каналы в одном волокне. Требования к синхронизации. Протоколы постобработки: коррекция ошибок (Cascade, LDPC), усиление приватности (Toeplitz-хеширование).
Тема 4. Постквантовая криптография (PQC)	Причины перехода на PQC. Основные семейства: на основе кодов (McEliece), на основе решеток (Kyber, Dilithium), на основе хэш-функций (SPHINCS+), многомерных систем. Сравнение с QKD. Конкурс NIST.

Тема 5. Квантовая криптография в корпоративной и государственной ИБ	Примеры внедрения: финансовый сектор (защита переводов), государственные сети, ЦОД. Отечественные разработки: НСЦ «Кулон», InfoWatch, QRate. Перспективы развития.
Тема 6. Будущее квантовых технологий в ИБ	Квантовый интернет. Распределенные квантовые вычисления. Устойчивость к квантовым атакам. Прогнозы развития. Обзор новейших исследований.
УП.08.01 Учебная практика (Квантовые коммуникации и квантовая криптография)	
Выполнение практических заданий по темам, изученным в МДК профессионального модуля. Закрепление освоенных навыков на учебных примерах	

6. Образовательные результаты освоения дисциплины (модуля):

Код и наименование компетенции	Результаты освоения дисциплины
ПК-01. Выполняет монтаж, настройку и администрирование сетевого оборудования и систем обеспечения информационной безопасности	ИПК-01.4. Реализует сетевую безопасность (межсетевые экраны, VPN, ACL, IDS/IPS)
ПК-03. Применяет программно-аппаратные средства и методы обеспечения информационной безопасности, включая тестирование на проникновение и анализ защищённости	ИПК-03.1. Применяет криптографические средства и методы защиты информации
ПК-04. Применяет средства автоматизации для администрирования, управления инцидентами и настройки систем информационной безопасности	ИПК-04.2. Осуществляет мониторинг и управление инцидентами в ИТ-системах
	ИПК-04.4. Применяет инструменты автоматизации для настройки средств защиты
ПК-07. Применяет методы математического анализа, дискретной математики и математической логики для построения моделей, разработки алгоритмов и анализа информационных систем в профессиональной деятельности	ИПК-07.5. Использует методы теории вероятностей и математической статистики для оценки надежности программных средств, обработки результатов экспериментов и анализа рисков в информационных системах
	ИПК-07.6. Применяет элементы теории алгоритмов и формальных языков (конечные автоматы, рекурсия, оценка сложности) для выбора оптимальных структур данных и разработки эффективных алгоритмов обработки информации
ПК-08. Применять основы квантовой криптографии и участвовать в эксплуатации систем квантового распределения ключей в защищённых телекоммуникационных сетях	ИПК-08.1. Знает физические принципы квантовых коммуникаций и основы квантовой криптографии
	ИПК-08.2. Описывает архитектуру и принцип работы систем квантового распределения ключей (КРК)

	ИПК-08.3. Выполняет базовую настройку и контроль параметров квантовой линии связи
	ИПК-08.4. Использует постреляционную обработку ключа для усиления секретности
	ИПК-08.5. Интегрирует квантовый ключ в классические системы шифрования