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 ПРАКТИКИ

«Производственная практика (по профилю специальности)»

1. Трудоемкость производственной практики (по профилю специальности): 432 ак.ч.

2. Место производственной практики (по профилю специальности) в учебном плане:

Производственная практика (по профилю специальности) входит в образовательный компонент программы ПП.00 «Практическая подготовка» (ПП.01) и является обязательной. Производственная практика (по профилю специальности) реализуется с 5 по 7 семестры.

3. Цель производственной практики (по профилю специальности): закрепление теоретических знаний и приобретение практических навыков в области обеспечения информационной безопасности телекоммуникационных систем, развитие компетенций для самостоятельного решения профессиональных задач.

4. Задачи производственной практики (по профилю специальности):

1. Ознакомительная задача: изучение структуры организации, её инфраструктуры и особенностей функционирования телекоммуникационной системы предприятия.
2. Информационно-аналитическая задача: анализ состояния информационной безопасности существующих телекоммуникационных систем и выявление потенциальных угроз и уязвимостей.
3. Проектная задача: разработка предложений по совершенствованию механизмов защиты информационных ресурсов телекоммуникационных систем предприятия.
4. Практико-ориентированная задача: реализация мероприятий по обеспечению информационной безопасности, включая настройку средств защиты информации, мониторинг и аудит сетевых инфраструктур.
5. Исследовательская задача: проведение исследований современных методов и технологий защиты информации применительно к специфике телекоммуникационных систем.
6. Методологическая задача: освоение методик оценки эффективности используемых средств защиты информации и разработки рекомендаций по повышению уровня защищенности сетей связи.
7. Документальная задача: составление отчетной документации по итогам прохождения практики, включающей описание выполненных работ, полученных результатов и выводов относительно состояния информационной безопасности телекоммуникационных систем.
8. Профессионально-коммуникативная задача: формирование навыков взаимодействия с техническими специалистами и руководством организации по вопросам обеспечения информационной безопасности телекоммуникационных систем.

5. Перечень разделов (тем) производственной практики (по профилю специальности) и их краткое содержание:

Наименование раздела (темы) практики	Краткое содержание
Раздел 1. Основы информационной безопасности	Ознакомление с существующей системой политики информационной безопасности на предприятии. Определение ключевых направлений развития корпоративной политики информационной безопасности. Оценка рисков нарушения конфиденциальности, целостности и доступности информации.

Раздел 2. Криптографические методы защиты информации	Настройка и проверка работоспособности основных криптографических протоколов и сервисов (SSL/TLS, IPsec). Аудит используемого программного обеспечения для шифрования и аутентификации. Тестирование стойкости используемых ключей шифрования.
Раздел 3. Организация защиты каналов передачи данных	Проектирование и настройка виртуальных частных сетей (VPN). Проверка надежности соединений и устойчивости к атакам типа MITM ("человек посередине"). Мониторинг активности сетевых интерфейсов и своевременное обнаружение аномалий трафика.
Раздел 4. Защита компьютерных сетей и телекоммуникационного оборудования	Установка и настройка брандмауэров различных типов (stateful firewall, proxy-firewall). Конфигурация правил фильтрации сетевого трафика. Применение IDS/IPS решений для обнаружения и предотвращения несанкционированного доступа.
Раздел 5. Управление доступом и идентификация пользователей	Создание базы данных учетных записей сотрудников и распределение ролей. Подключение биометрической системы идентификации пользователей (например, сканеры отпечатков пальцев, лица). Ревизия прав доступа и журналов авторизации.
Раздел 6. Сертификация и лицензирование в области информационной безопасности	Участие в проведении аудита сертифицированных продуктов и процессов.
Раздел 7. Инцидент-менеджмент и кризисное управление	Разработка плана реагирования на чрезвычайные ситуации, связанный с нарушением безопасности сети. Отработка сценария ликвидации последствий инцидента, вызванного вирусным заражением серверов или утечкой данных. Совершенствование процедур анализа и фиксации происшествий, связанных с нарушениями безопасности телекоммуникационных систем.
Раздел 8. Операционные системы и инфраструктура вычислительных платформ	Выполнение установки и настройки операционной системы сервера Windows Server / Linux. Настройка стандартных служб ОС (DNS, DHCP, AD, File Services и др.). Администрирование кластеров виртуализации (VMware vSphere, Hyper-V, KVM). Оптимизация производительности серверов и виртуальной среды.
Раздел 9. Сети и сетевое оборудование	Построение схемы ЛВС и определение требований к оборудованию. Настройка коммутаторов, роутеров и точек доступа Wi-Fi. Диагностика проблем в сетях и устранение неисправностей. Обеспечение безопасности сетей (VRF, ACL, NAT).

Раздел 10. Базы данных и СУБД	Установка и конфигурирование популярных СУБД (MySQL, PostgreSQL, MS SQL Server). Написание запросов на выборку и изменение данных. Резервное копирование и восстановление баз данных. Мониторинг производительности СУБД и оптимизация индексов таблиц.
Раздел 11. Автоматизация и мониторинг ИТ-сервисов	Использование инструментов автоматизации (Ansible, Puppet, Chef). Установка и настройка систем мониторинга (Zabbix, Nagios, Prometheus). Постановка регулярных заданий резервного копирования. Автоматизация рутинных операций администрирования.
Раздел 12. Сервисы и приложения	Установка и настройка серверов приложений (Apache Tomcat, JBoss, IIS). Интеграция web-приложений с внешними сервисами (API). Миграция приложений в облако и развертывание в среде контейнеризации (Docker/Kubernetes). Обслуживание почтового сервиса (MS Exchange, Postfix/Dovecot).
Раздел 13. Средства охранной сигнализации	Выбор и расчет количества датчиков движения, вибрации, открытия дверей окон и иных элементов системы сигнализации. Монтаж, подключение и тестирование датчиков охранной сигнализации. Наладка чувствительности и зон покрытия сигнализационных устройств.
Раздел 14. Средства видеонаблюдения	Установка камер видеонаблюдения разного типа (IP-камер, аналоговых, PTZ-камер). Прокладка кабелей питания и передачи сигнала. Настройка видеорегистраторов и серверов видеонаблюдения. Интеграция видеосистемы с остальными элементами системы физической защиты.
Раздел 15. Средства контроля и управления доступом	Расчет пропускной способности турникетов и шлагбаумов. Установка считывающих устройств (карточек, биометрии, PIN-кодов). Программирование контроллеров СКУД и интеграция с общей системой безопасности. Диагностика и ремонт исполнительных механизмов.

6. Образовательные результаты освоения практики:

Код и наименование компетенции	Результаты освоения практики
ЛК-01. Выбирает способы решения задач профессиональной	ИЛК-01.4. Адаптируется к изменяющимся условиям и новым идеям, корректирует способы действий на основе переоценки накопленного опыта и прогнозирования изменений

деятельности применительно к различным контекстам	ИЛК-01.5. Реализует составленный план, эффективно выполняя несколько разноплановых профессиональных задач без потери качества
	ИЛК-01.6. Оценивает результат решения задачи и последствия своих действий (самостоятельно или с помощью наставника), применяя установленный порядок оценки результатов профессиональной деятельности
ЛК-04. Эффективно взаимодействует и работает в коллективе и команде	ИЛК-04.5. Анализирует производственную ситуацию и называет противоречия между реальными и идеальными условиями реализации технологического процесса
ЛК-05. Осуществляет устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	ИЛК-05.4. Знает особенности социального и культурного контекста, проявляет толерантность в рабочем коллективе
ПК-01. Выполняет монтаж, настройку и администрирование сетевого оборудования и систем обеспечения информационной безопасности	ИПК-01.1. Выполняет установку и конфигурирование аппаратного обеспечения ПК, серверов и периферийного оборудования
	ИПК-01.2. Выполняет монтаж и подключение линейных сооружений связи и кабельных систем
	ИПК-01.3. Администрирует сетевые устройства (маршрутизаторы, коммутаторы)
	ИПК-01.4. Реализует сетевую безопасность (межсетевые экраны, VPN, ACL, IDS/IPS)
	ИПК-01.5. Осуществляет аудит безопасности и контроль целостности вычислительной системы
ПК-02. Обеспечивает бесперебойное функционирование, мониторинг и защиту сетевой инфраструктуры	ИПК-02.1. Обеспечивает мониторинг доступности сетевых устройств и каналов связи
	ИПК-02.2. Настраивает протоколы динамической маршрутизации (OSPF, RIP) и управление пропускной способностью каналов связи
	ИПК-02.3. Проводит анализ журналов событий (syslog, SNMP) для выявления сбоев
	ИПК-02.4. Обеспечивает резервирование и отказоустойчивость сетевой инфраструктуры
	ИПК-02.5. Анализирует сетевой трафик и выявляет инциденты информационной безопасности

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
	ИПК-03.2. Способен устанавливать и конфигурировать программно-аппаратные средства защиты информации
	ИПК-03.3. Выполняет тестирование на проникновение и анализ защищённости
	ИПК-03.4. Анализирует уязвимости и составляет отчёты по результатам тестирования
	ИПК-03.5. Обеспечивает антивирусную защиту и контроль программного обеспечения
ПК-04. Применяет средства автоматизации для администрирования, управления инцидентами и настройки систем информационной безопасности	ИПК-04.1. Разрабатывает скрипты для автоматизации задач администрирования и безопасности
	ИПК-04.2. Осуществляет мониторинг и управление инцидентами в ИТ-системах
	ИПК-04.3. Работает в системах Service Desk и управления конфигурациями
	ИПК-04.4. Применяет инструменты автоматизации для настройки средств защиты
ПК-05. Обеспечивает физическую и техническую защиту объектов информатизации, включая выявление и блокирование каналов утечки информации	ИПК-05.1. Организует физическую защиту объектов информатизации (СКУД, видеонаблюдение)
	ИПК-05.2. Выявляет и блокирует технические каналы утечки информации
	ИПК-05.3. Обеспечивает электробезопасность и защиту от электромагнитных излучений
	ИПК-05.4. Эксплуатирует инженерно-технические средства охраны
ПК-06. Использует знания в области информатики и информационных технологий в профессиональной деятельности	ИПК-06.1. Применяет прикладные офисные пакеты в профессиональной деятельности
	ИПК-06.2. Использует блок-схемы для описания алгоритмов
	ИПК-06.3. Знает и использует операции алгебры логики в профессиональной деятельности
	ИПК-06.4. Работает с численными значениями, представленными в разных системах счисления
	ИПК-06.5. Знает и использует основные понятия теории информации

ПК-07. Применяет методы математического анализа, дискретной математики и математической логики для построения моделей, разработки алгоритмов и анализа информационных систем в профессиональной деятельности	ИПК-07.1. Выполняет операции над матрицами, решает системы линейных уравнений и использует элементы теории множеств и комбинаторики для формализации задач обработки данных и разработки алгоритмов
	ИПК-07.2. Применяет методы дифференциального и интегрального исчисления для анализа характеристик процессов (скорость передачи данных, оптимизация алгоритмов, моделирование систем)
	ИПК-07.3. Использует алгебру логики для построения сложных условий, оптимизации логических выражений, формирования запросов к базам данных и разработки алгоритмов принятия решений
	ИПК-07.4. Применяет теорию графов для моделирования структур данных (сети, деревья решений, схемы баз данных, иерархии) и оптимизации маршрутов обработки информации
	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