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

## «Сетевая инфраструктура и кибербезопасность»

**1. Трудоемкость профессионального модуля:** 342 ак.ч.

**2. Место профессионального модуля в учебном плане:**

Профессиональный модуль «Сетевая инфраструктура и кибербезопасность» входит в образовательный компонент программы П.00 «Профессиональный цикл» (ПМ.05) и является вариативным. Профессиональный модуль реализуется в 3-5 семестрах.

**3. Цель профессионального модуля:** формировать у обучающихся профессиональные компетенции для проектирования, монтажа, администрирования и защиты сетевой инфраструктуры с применением современных сетевых технологий и протоколов, обеспечивающих надёжность и кибербезопасность информационных систем.

**4. Задачи профессионального модуля:**

– освоить принципы проектирования сетевой инфраструктуры: изучить современные сетевые технологии и протоколы (TCP/IP, OSPF, BGP, VLAN, VPN и др.), научиться разрабатывать схемы сетей с учётом требований к производительности и безопасности;

– приобрести практические навыки монтажа и настройки сетевого оборудования (маршрутизаторов, коммутаторов, межсетевых экранов): выполнить подключение, базовую конфигурацию и тестирование работоспособности устройств от ведущих производителей (Cisco, Juniper, Huawei и аналогичных);

– овладеть навыками администрирования сетевых сервисов и инфраструктуры: научиться управлять DHCP, DNS, NTP и другими сетевыми службами, мониторить трафик и производительность сети, оперативно устранять возникающие неполадки;

– изучить методы и инструменты защиты сетевой инфраструктуры: освоить настройку межсетевых экранов, систем обнаружения и предотвращения вторжений (IDS/IPS), организовать сегментацию сети и контроль доступа, реализовать шифрование трафика (IPsec, SSL/TLS);

– развить компетенции по анализу угроз и реагированию на инциденты кибербезопасности: научиться выявлять признаки атак (DDoS, MITM, сканирование портов и т.д.), анализировать логи сетевого оборудования и средств защиты, разрабатывать и применять планы реагирования на инциденты, проводить аудит безопасности сети.

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

| Наименования разделов (тем) профессионального модуля | Содержание разделов (тем) профессионального модуля |
|---|---|
| **МДК.05.01 Архитектура, монтаж и конфигурация компьютерных сетей** | |
| Тема 1. Классификация и топологии сетей | Локальные, городские, глобальные сети. Топологии: звезда, шина, кольцо, ячеистая, древовидная. Выбор топологии в зависимости от задач. |
| Тема 2. Структурированные кабельные системы (СКС) | Кабели: витая пара (UTP, FTP, категории 5e, 6, 6a, 7), оптоволокно (одномодовое, многомодовое). Коннекторы (RJ-45, SC, LC). Обжим и тестирование кабелей. Патч-панели, коммутационные шкафы. Стандарты TIA/EIA 568. |

| | |
|---|---|
| Тема 3. Сетевое оборудование | Сетевые адаптеры (NIC). Повторители, концентраторы (Hub). Коммутаторы (Switch): управляемые и неуправляемые. Маршрутизаторы (Router). Точки доступа Wi-Fi. Принципы работы на L1, L2, L3. |
| Тема 4. Коммутация и виртуальные сети (VLAN) | Принцип коммутации. MAC-таблица. VLAN: назначение, статические и динамические. Тегирование 802.1Q. Trunk-порты. |
| Тема 5. Протоколы STP и EtherChannel | Проблема петель. Spanning Tree Protocol (STP, RSTP, MSTP). Алгоритм выбора корневого моста. EtherChannel (LACP, PAgP). |
| Тема 6. Беспроводные сети | Стандарты 802.11 (a/b/g/n/ac/ax). Режимы: Ad-hoc, Infrastructure. Безопасность Wi-Fi (WPA2-PSK, WPA3, 802.1X). |
| **МДК.05.02 Администрирование сетевых устройств и протоколы маршрутизации** | |
| Тема 1. Основы маршрутизации | Таблица маршрутизации. Статическая маршрутизация. Маршрут по умолчанию. Динамическая маршрутизация: дистанционно-векторные и Link-state протоколы. |
| Тема 2. Протокол RIP | RIP v1 и v2. Метрика — хопы. Таймеры. Ограничения RIP. |
| Тема 3. Протокол OSPF | OSPF как Link-state протокол. Зоны (area) и области. DR/BDR. Hello-протокол. Метрика cost. |
| Тема 4. Протокол BGP (обзор) | Внешняя маршрутизация. AS (Autonomous System). eBGP и iBGP. Атрибуты. Применение в магистралях. |
| Тема 5. DHCP и DNS | Протокол DHCP (DORA). Relay. Статические и динамические назначения. DNS: рекурсивные и авторитетные запросы. Типы записей (A, AAAA, CNAME, MX, PTR). |
| Тема 6. NAT | Static NAT, Dynamic NAT, PAT (Port Address Translation). Назначение — экономия IPv4-адресов. |
| **МДК.05.03 Сетевая безопасность (Межсетевые экраны, VPN, ACL, IDS/IPS)** | |
| Тема 1. Списки контроля доступа (ACL) | Стандартные и расширенные ACL. Нумерованные и именованные. Правила фильтрации по IP, портам, протоколам. Применение на интерфейсах (in/out). |
| Тема 2. Межсетевые экраны (МЭ) | Классификация: пакетные фильтры, statefull (сессионные), проксирующие, NGFW. iptables/nftables (Linux), MikroTik Firewall, Cisco ACL/Zone-based Firewall. Правила цепочек (INPUT, OUTPUT, FORWARD). |
| Тема 3. Технологии VPN | Виды VPN: Site-to-Site, Remote Access. Протоколы: IPsec (IKE, ESP, AH), OpenVPN (SSL/TLS), WireGuard, PPTP (устаревший). |
| Тема 4. Системы обнаружения вторжений (IDS/IPS) | Подходы: сигнатурный, поведенческий, аномалийный. Примеры: Snort, Suricata, Zeek (Bro). Расположение: inline (IPS) и out-of-band (IDS). |
| Тема 5. Защита от атак сетевого уровня | Защита от ARP-spoofing, DHCP-атак (DHCP snooping), атак на STP (BPDU guard, Root guard), VLAN hopping (VLAN access map). |
| **МДК.05.04 Сетевые протоколы, иерархия открытых систем OSI и стек протоколов TCP/IP** | |

| | |
|---|---|
| Тема 1. Модель OSI | 7 уровней OSI: физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной. Функции каждого уровня. Инкапсуляция и деинкапсуляция. |
| Тема 2. Стек протоколов TCP/IP | 4 уровня: сетевых интерфейсов, интернет (IP), транспортный (TCP/UDP), прикладной. Сравнение с OSI. |
| Тема 3. Протокол IP (IPv4, IPv6) | IPv4: структура заголовка, фрагментация, TTL. Адресация (классы, CIDR, подсети). IPv6: структура заголовка, адресация (link-local, global unicast, multicast). |
| Тема 4. Протоколы транспортного уровня: TCP и UDP | TCP: трехстороннее рукопожатие, окно, подтверждения. Порты. UDP: простота, ненадежность. Сравнение. |
| Тема 5. Прикладные протоколы | HTTP/HTTPS (методы, коды ответа), FTP (active/passive), SMTP, POP3, IMAP, Telnet, SSH. |
| Тема 6. Анализ сетевого трафика с Wireshark/tcpdump | Захват трафика. Фильтры (по IP, порту, протоколу). Статистика. Следование потока TCP. |
| **УП.05.01 Учебная практика (Сетевая инфраструктура и кибербезопасность)** | |
| 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 |
|---|---|
| ЛК-05. Осуществляет устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста | ИЛК-05.1. Применяет современную терминологию на государственном языке, относящуюся к описанию предметов, средств и процессов профессиональной деятельности |
| ПК-01. Выполняет монтаж, настройку и администрирование сетевого оборудования и систем обеспечения информационной безопасности | ИПК-01.3. Администрирует сетевые устройства (маршрутизаторы, коммутаторы) |
| | ИПК-01.4. Реализует сетевую безопасность (межсетевые экраны, VPN, ACL, IDS/IPS) |
| ПК-02. Обеспечивает бесперебойное функционирование, мониторинг и защиту сетевой инфраструктуры | ИПК-02.3. Проводит анализ журналов событий (syslog, SNMP) для выявления сбоев |