АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. Эксплуатация объектов сетевой инфраструктуры

название профессионального модуля

1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности «Эксплуатация объектов сетевой инфраструктуры» и соответствующие ему профессиональные компетенции и общие компетенции:

Перечень общих компетенций

Код	**Наименование общих компетенций**
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.
ОК 11.	Планировать предпринимательскую деятельность в профессиональной сфере

Перечень профессиональных компетенций

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 3.	*Эксплуатация объектов сетевой инфраструктуры*
ПК 3.1	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
ПК 3.2	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
ПК 3.3.	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.
ПК 3.5.	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.

ПК 3.6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

В результате освоения профессионального модуля студент должен:

Иметь практический опыт в	обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя; удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры; поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры *Внедрять механизмы сетевой безопасности на втором уровне модели OSI.* *Внедрять механизмы сетевой безопасности с помощью межсетевых экранов.* *Внедрять технологии VPN.* *Настраивать IP-телефоны* *Выполнять профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.* *Составлять план-график профилактических работ.* *Обеспечивать защиту сетевых устройств.*
уметь	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; осуществлять диагностику и поиск неисправностей всех компонентов сети; выполнять действия по устранению неисправностей *Описывать современные технологии и архитектуры безопасности.* *Описывать характеристики и элементы конфигурации этапов VoIP звонка.* *Устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту.* *Описывать концепции сетевой безопасности.* *Наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных.*
знать	архитектуру и функции систем управления сетями, стандарты систем управления; средства мониторинга и анализа локальных сетей; методы устранения неисправностей в технических средствах *Основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.* *Принципы работы сети аналоговой телефонии.* *Назначение голосового шлюза, его компоненты и функции.* *Основные принципы технологии обеспечения QoS для голосового трафика сетей.* *Основные понятия, средства мониторинга и анализа локальных сетей.* *Методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных.*

2.Количество часов, отводимое на освоение профессионального модуля

Всего часов – 608 часов, в том числе:

- 274 часа вариативной части, направленных на усиление обязательной части программы профессионального модуля.

3. Содержание профессионального модуля

МДК 03.01 Эксплуатация объектов сетевой инфраструктуры

Тема 1. Эксплуатация технических средств сетевой инфраструктуры

Тема 2. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях.

Тема 3. Эксплуатация систем IP-телефонии.

Тема 4. Средства мониторинга и анализа локальных сетей

Тема 5. Хранение информации в информационной системе

Тема 6. Схема после аварийного восстановления

Тема 7. Замена расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры

МДК.03.02. Безопасность компьютерных сетей

Тема 1. Проблемы информационной безопасности

Тема 2. Технологии защиты данных

Тема 3. Технологии защиты межсетевого обмена данными.

Тема 4. Технологии обнаружения вторжений

Тема 5. Управление сетевой безопасностью

Учебная практика

1. Настройка прав доступа.
2. Оформление технической документации, правила оформления документов.
3. Настройка аппаратного и программного обеспечения сети.
4. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.
5. Программная диагностика неисправностей.
6. Аппаратная диагностика неисправностей.
7. Поиск неисправностей технических средств.
8. Выполнение действий по устранению неисправностей.
9. Использование активного, пассивного оборудования сети.
10. Устранение паразитирующей нагрузки в сети.
11. Построение физической карты локальной сети.
12. Исследование сетевых атак и инструментов проверки защиты сети
13. Настройка безопасного доступа к маршрутизатору
14. Обеспечение административного доступа AAA и сервера Radius
15. Настройка политики безопасности брандмауэров
16. Настройка системы предотвращения вторжений (IPS)
17. Настройка безопасности на втором уровне на коммутаторах
18. Исследование методов шифрования

Производственная практика

1. Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение.
2. Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях.

3. Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций.

4. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли.

5. Установка прав доступа и контроль использования сетевых ресурсов.

6. Обеспечение своевременного копирования, архивирования и резервирования данных.

7. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования.

8. Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению.

9. Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети.

10. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.

11. Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций.

12. Документирование всех произведенных действий.

13. Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации.

14. Разработка политик безопасности и внедрение их в операционные системы.

15. Настройка IPSec и VPN. Настройка межсетевых экранов.

16. Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств.

17. Настройка защиты беспроводных сетей с помощью систем шифрования.

18. Архивация и восстановление ключей в WindowsServer (PKI).