**МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ**

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**РОСТОВСКОЙ ОБЛАСТИ**

**«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ СВЯЗИ И ИНФОРМАТИКИ»**

|  |  |
| --- | --- |
|  |  |

**РАБОЧАЯ ПРОГРАММА**

**УЧЕБНОЙ ПРАКТИКИ**

**УП 03.01 Защита информации**

Специальности среднего профессионального образования

**11.02.15 «Инфокоммуникационные сети и системы связи»**

(базовой подготовки)

Ростов-на-Дону

2025г.

|  |  |
| --- | --- |
| **ОДОБРЕНО**  На заседании цикловой комиссии  Телекоммуникаций  Протокол № 7 от 05.02 .2025.  Председатель ЦК  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Л.В.Ермолина | **СОГЛАСОВАНО**  Зам. директора по УПР и ИБ  ГБПОУ РО «РКСИ»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.В. Коваленко  «\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_2025г. |

Рабочая программа учебной практики разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 11.02.15 «Инфокоммуникационные сети и системы связи» и Положения о практической подготовке обучающихся, осваивающих образовательные программы среднего профессионального образования от 5 августа 2022 г. N 675

Организация-разработчик: Государственное бюджетное образовательное учреждение среднего профессионального образования Ростовской области «Ростовский-на-Дону колледж связи и информатики».

Разработчик: УП.03.01 – Бойнар И.Н., преподаватель специальных дисциплин ГБПОУ РО «РКСИ».

**СОДЕРЖАНИЕ**

1. Паспорт программы учебной практики 4

2. Результаты освоения программы учебной практики 6

3. Тематический план и содержание учебной практики 7

4. Условия реализации программы учебной практики 9

5. Контроль и оценка результатов освоения учебной практики 11

**1 ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ**

* 1. **Область применения программы**

Рабочая программа учебной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 11.02.15 «Инфокоммуникационные сети и системы связи» в части освоения квалификации «Техник» и основных видов профессиональной деятельности (ВПД):

* анализ сетевой инфраструктуры;
* выявление угроз и уязвимости в сетевой инфраструктуре;
* разработка комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;
* осуществление текущего администрирования для защиты инфокоммуникационных сетей и систем связи;
* использование специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.

**1.2 Цели и задачи учебной практики**

Учебная практика по специальности направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках профессионального модуля ППССЗ СПО по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по избранной специальности.

**1.3 Требования к результатам освоения учебной практики**

В результате прохождения учебной практики по видам профессиональной деятельности обучающийся должен **уметь:**

в области обеспечения информационной безопасности инфокоммуникационных сетей и систем связи:

* классифицировать угрозы информационной безопасности;
* проводить выбор средств защиты в соответствии с выявленными угрозами;
* определять возможные виды атак;
* использовать программные продукты, выявляющие недостатки систем защиты;
* выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
* производить установку и настройку средств защиты;
* конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
* выполнять тестирование систем с целью определения уровня защищенности;
* применять криптографические методы защиты информации;

**1.3. Количество часов на освоение рабочей программы учебной практики**

*Всего - 36 часов, в том числе:*

*В рамках освоения ПМ .03 - 36 часов*

**2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ**

*Результатом освоения рабочей программы учебной практики является форсированность у обучающихся первоначальных практических профессиональных* ***умений*** *в рамках модуля* ППССЗ *СПО по виду профессиональной деятельности (ВПД):*

* обеспечение информационной безопасности инфокоммуникационных сетей и систем связи;

*необходимых для последующего освоения ими общих (ОК) и профессиональных (ПК) компетенций по избранной профессии.*

|  |  |
| --- | --- |
| ***Код*** | ***Наименование результата освоения практики*** |
| Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи | |
| ПК 3.1 | Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. |
| ПК 3.2 | Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. |
| ПК 3.3 | Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. |
| Общие компетенции | |
| ОК 1 | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам |
| ОК 2 | Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности |
| ОК 3 | Планировать и реализовывать собственное профессиональное личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях |
| ОК 4 | Эффективно взаимодействовать и работать в коллективе и команде |
| ОК 5 | Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста |
| ОК 6 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения; |
| ОК 7 | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях |
| ОК 8 | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности |
| ОК 9 | Пользоваться профессиональной документацией на государственном и иностранном языках |

**3 ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ**

**3.1 Тематический план учебной практики**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Код  ПК | Код и наименования профессиональных модулей | Количество  часов по ПМ | Виды работ | Наименования тем учебной практики | Кол-во  часов  по  темам |
| ПМ03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи | | | | | |
| ПК 3.1 – 3.3 | ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи | 36 | - установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов;  - установка и настройка типовых программно-аппаратных средств защиты информации;  - использование программно-аппаратных и инженерно-технических средств.  - настройка, регулировка и ремонт оборудования средств защиты;  - выбор способов и средств   многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой;  - проведение типовых операции настройки средств защиты операционных систем;  - проведение аттестации объектов защиты;  - определение источников несанкционированного доступа, исходя из модели угроз;  - определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта;  - обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств;  - защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК;   * - защита информации организационными методами в соответствии с инструкциями на объекте. | Тема 1.1 Установка и настройка средств технической защиты информации | 10 |
| Тема 1.2 Анализ защищенности ТКС | 16 |
| Тема 1.3 Защита информации в корпоративной сети | 10 |
| Промежуточная аттестация в форме  зачета |  |

**3.2. Содержание учебной практики**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Код и  наименование  профессиональных  модулей и тем  учебной практики | Содержание учебных занятий | | Объем  часов | | Уровень  освоения |
| ***1*** | ***2*** | | ***3*** | | ***4*** |
| ПМ03 **Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи** | | | | | |
| УП 03.01 «Защита информации» | | | | **36** |  |
| **Виды работ:**  - установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов;  - установка и настройка типовых программно-аппаратных средств защиты информации;  - использование программно-аппаратных и инженерно-технических средств.  - настройка, регулировка и ремонт оборудования средств защиты;  - выбор способов и средств   многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой;  - проведение типовых операции настройки средств защиты операционных систем;  - проведение аттестации объектов защиты;  - определение источников несанкционированного доступа, исходя из модели угроз;  - определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта;  - обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств;  - защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК;  - защита информации организационными методами в соответствии с инструкциями на объекте. | | | | | |
| Тема 1 Установка и настройка средств технической защиты информации | Содержание | | **10** | |  |
| 1 | Определение способов и средств   многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой | 2 | | ***3*** |
| 2 | Технические средства защиты информации и средства охраны объектов | 4 | | ***3*** |
|  | 3 | Настройка и использование инженерно-технических средств защиты информации | 4 | | ***3*** |
| Тема 2 Анализ защищенности ТКС | Содержание | | **16** | |  |
| 1 | Установка и настройка программно-аппаратных средств защиты информации от НСД | 6 | | ***3*** |
| 2 | Настройка средств сканирования сети на определение уязвимостей | 6 | | ***3*** |
|  | 3 | Резервное копирование данных | 2 | | ***3*** |
|  | 4 | Основные принципы работы с антивирусными программами | 2 | | ***3*** |
| Тема 3 Защита информации в корпоративной сети | Содержание | | **10** | |  |
| 1 | Создание и управление компонентами виртуальной сети | 4 | | ***3*** |
| 2 | Настройка межсетевого соединения | 4 | | ***3*** |
| 3 | Применения политик безопасности в виртуальной среде | 2 | | ***3*** |
| ***Промежуточная аттестация в форме зачета*** | | | |  |  |

**4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ**

**4.1 Требования к минимальному материально-техническому обеспечению.**

Учебная практика проводится в учебных, учебно-производственных мастерских, лабораториях колледжа.

4.1.1 Для реализации рабочей программы учебной практики необходимы следующие ресурсы:

лаборатории:

* «Сетей передачи данных»;
* «Информационной безопасности телекоммуникационных систем»

Учебная практика реализуется в мастерских профессиональной образовательной организации и требует наличия оборудования, инструментов, расходных материалов, обеспечивающих выполнение всех видов работ, определенных содержанием программ профессиональных модулей, в том числе оборудования и инструментов, используемых при проведении чемпионатов Профессионалы и указанных в инфраструктурных листах конкурсной документации Профессионалы по компетенциям «Информационные кабельные сети», Корпоративная защита от внутренних угроз информационной безопасности» (или их аналогов).

4.1.2 Оборудование:

* компьютеры в комплекте (системный блок, монитор, клавиатура, манипулятор «мышь») или ноутбуки (моноблоки),
* программно-аппаратный межсетевой экран (комплекс сетевой защиты)
* комплекс антивирусного программного обеспечения,
* комплекс программного обеспечения шифрования и дешифрования данных с использованием различных систем шифрования,
* устройства защиты слаботочных систем коммуникаций (телефонная линия, радиотрансляция)

4.1.4 Средства обучения:

* компьютеры с лицензионным программным обеспечением и мультимедиа проектор;
* локальная сеть с выходом в Интернет,
* учебно-методическое обеспечение:

электронные УМК, отраслевые стандарты, Приказы ФСТЭК №21, №17, №239, инструкции по эксплуатации средств защиты информации.

**4.2 Кадровое обеспечение и требования к организации образовательного процесса**

4.2.1 Учебная практика проводится преподавателями дисциплин профессионального цикла, являющимися сотрудниками Колледжа, имеющими высшее образование, соответствующее профилю преподаваемого модуля, (указать характер проведения учебной практики: рассредоточено/концентрированно).

4.2.1 Преподаватели должны проходить обязательную стажировку в профильных организациях не реже 1-го раза в 3 года.

**5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ**

**УЧЕБНОЙ ПРАКТИКИ**

Контроль и оценка результатов освоения учебной практики осуществляется преподавателем в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических работ с обязательной фиксацией результатов промежуточного и итогового контроля в журнале группы.

При необходимости группа может делиться на бригады от 3 до 5 человек для выполнения практических работ на оборудовании.

В результате освоения учебной практики в рамках профессиональных модулей обучающиеся проходят промежуточную аттестацию в форме **зачета.**

|  |  |
| --- | --- |
| ***Результаты обучения (освоенные умения в рамках ВПД)*** | ***Формы и методы контроля и***  ***оценки результатов обучения*** |
| Классифицирует угрозы информационной безопасности | Экспертная оценка результатов при выполнении работ на различных этапах учебной практики |
| Проводит выбор средств защиты в соответствии с выявленными угрозами | Экспертная оценка результатов при выполнении работ на различных этапах учебной практики |
| Определяет возможные виды атак | Экспертная оценка результатов при выполнении работ на различных этапах учебной практики |
| Выполняет расчет и установку специализированного оборудования для максимальной защищенности объекта. | Экспертная оценка результатов при выполнении работ на различных этапах учебной практики |
| Применяет криптографические методы защиты информации | Экспертная оценка результатов при выполнении работ на различных этапах учебной практики |