АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Рабочая программа учебной практики (по профилю специальности) (далее рабочая программа) – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности ***11.02.15 Инфокоммуникационные сети и системы связи (углубленной подготовки)*** в части освоения основного вида профессиональной деятельности (ВПД): **Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи** и соответствующих профессиональных компетенций (ПК):

1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.
3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.

Рабочая программа учебной практики может быть использована в дополнительном профессиональном образовании, профессиональной подготовке работников в области монтажа, эксплуатации и технического обслуживания телекоммуникационного оборудования при наличии среднего (полного) общего образования. Опыт работы не требуется.

1.2. Цели и задачи учебной практики – требования к результатам освоения учебной практики:

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной практики должен:

иметь практический опыт:

- выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности;
- разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;
- осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.

уметь:

- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;

определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;

осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;

выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты
выполнять тестирование систем с целью определения уровня защищенности;
определять оптимальные способы обеспечения информационной безопасности;
проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;
проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;
разрабатывать политику безопасности сетевых элементов и логических сетей;
выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;
конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
защищать базы данных при помощи специализированных программных продуктов;
защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.
знать:
- принципы построения информационно-коммуникационных сетей;
международные стандарты информационной безопасности для проводных и беспроводных сетей;
нормативно - правовые и законодательные акты в области информационной безопасности;
акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;
технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
способы и методы обнаружения средств съёма информации в радиоканале;
классификацию угроз сетевой безопасности;
характерные особенности сетевых атак;
возможные способы несанкционированного доступа к системам связи;
правила проведения возможных проверок согласно нормативных документов ФСТЭК;
этапы определения конфиденциальности документов объекта защиты;
назначение, классификацию и принципы работы специализированного оборудования;
методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;
методы и средства защиты информации в телекоммуникациях от вредоносных программ;
технологии применения программных продуктов;
возможные способы, места установки и настройки программных продуктов;

методы и способы защиты информации, передаваемой по кабельным направляющим системам;
конфигурации защищаемых сетей;
алгоритмы работы тестовых программ;
средства защиты различных операционных систем и среды передачи информации;
способы и методы шифрования (кодирование и декодирование) информации.

1.3. Количество часов на освоение рабочей программы учебной практики:

на учебную практику отводится 72 часа (2 недели).