

Министерство образования и науки РИ
Государственное бюджетное профессиональное
образовательное учреждение
«Колледж сервиса и быта»

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
Специальности 10.02.04. Обеспечение информационной
безопасности телекоммуникационных систем
Квалификация – техник по защите информации

Составитель: Ахильгов Ю.А.

Назрань

2020г.

Рабочая программа профессионального модуля ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.04. Обеспечение информационной безопасности телекоммуникационных систем, утвержденный приказом Минобрнауки РФ от 9 декабря 2016 №1551 (зарегистрирован Министерством юстиции Российской Федерации от 26 декабря 2016 г. № 44944)

Организация-разработчик: ГБПОУ «КСИБ»

Разработчик: Ахильгов Ю. преподаватель ГБПОУ «КСИБ»

Программа рассмотрена на заседании кафедры общепрофессиональных и специальных дисциплин

Протокол № _____ от « ____ » _____ 20__ г.

Зав. кафедрой _____ /Р.А.Ажигова/

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
Специальности 10.02.04. Обеспечение информационной безопасности
телекоммуникационных систем
Квалификация – техник по защите информации

1. Область применения программы

Рабочая программа является частью ППССЗ специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

2. Место производственной практики в структуре образовательной программы:

Производственная практика относится к профессиональному циклу, проводится концентрировано в 3.,4,5,6 семестрах в объеме 576 ч.

Производственная практика направлена на формирование у обучающихся общих и профессиональных компетенций, приобретения практического опыта и реализуется в рамках профессиональных модулей: ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей, ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты, ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, ПМ.04 Освоение одной или нескольких профессий рабочих, должностей служащих по видам деятельности:

- эксплуатация информационно-телекоммуникационных систем и сетей;
- защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты;
- защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты.
- освоение одной или нескольких профессий рабочих, должностей служащих, предусмотренных ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

3. Показатели освоения программы производственной практики

Результатом освоения программы производственной практики является овладение обучающимися видами деятельности:

- эксплуатация информационно-телекоммуникационных систем и сетей;
- защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты;
- защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты;
- освоение одной или нескольких профессий рабочих, должностей служащих, необходимых для последующего освоения ими общих (ОК) и профессиональных (ПК) компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке

с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей.

ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей.

ПК 1.3. Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей.

ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.

ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно-телекоммуникационных систем и сетей.

ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.

ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.

ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.

ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

В результате освоения дисциплины обучающийся должен **иметь практический опыт**:

О1 – монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (ИТКС); О2 – текущего контроля функционирования оборудования ИТКС;

О3 – проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС;

О4 – применения программно-аппаратных средств обеспечения информационной безопасности;

О5 – диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;

О6 – мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;

О7 – обеспечение учета, обработки, хранения и передачи конфиденциальной информации;

О8 – решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;

О9 – применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами.
О10 – выявление технических каналов утечки информации;
О11 – использование основных методов и средств инженерно-технической защиты информации;
О12 – диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;
О13 – участие в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности;
О14 – решение частных технических задач, возникающих при аттестации объектов, помещений, технических средств.
О15 – выполнения технологического процесса сборки, монтажа и демонтажа узлов, блоков, приборов и устройств радиоэлектронной аппаратуры в соответствии с технической документацией;

В результате изучения профессионального модуля обучающийся должен **уметь**:

У1 – осуществлять техническую эксплуатацию линейных сооружений связи; У2 – производить монтаж кабельных линий и оконечных кабельных устройств; У3 – настраивать, эксплуатировать и обслуживать оборудование ИТКС;
У4 – осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС; У5 – производить испытания, проверку и приемку оборудования телекоммуникационных систем;

У6 – проводить работы по техническому обслуживанию, диагностики технического состояния и ремонту оборудования ИТКС; У7 – измерять основные качественные показатели и характеристики при выполнении профилактических и ремонтных работ приемо-передающих устройств (ППУ);
У8 – читать принципиальные схемы блоков ППУ;
У9 – выполнять расчеты, связанные с определением значений параметров режима и элементов ППУ; У10 – контролировать работу и осуществлять техническую эксплуатацию ППУ;
У11 – настраивать, эксплуатировать и обслуживать локальные вычислительные сети;
У12 – сопрягать между собой различные телекоммуникационные устройства;
У13 – производить настройку программного обеспечения коммутационного оборудования телекоммуникационных систем;
У14 – осуществлять настройку модемов, используемых в защищенных телекоммуникационных системах; У15 – проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры;
У16 – проводить типовые измерения;
У17 – пользоваться стандартными средствами электрорадиоизмерений;
У18 – оценивать точность проводимых измерений; У19 – оформлять эксплуатационную и ремонтную документацию.
У20 – применять программно-аппаратные средства обеспечения информационной безопасности;
У21 – диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
У22 – оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
У23 – участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;

- У24 – решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;
- У25 – использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;
- У26 – применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами.
- У27 – применять технические средства защиты информации;
- У28 – использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
- У29 – использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам;
- У30 – применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами.
- У31 – читать маркировку электрорадиоэлементов. читать электрические принципиальные схемы.
- У32 – пользоваться технологической документацией при изготовлении радиоэлектронной аппаратуры;
- У33 – формировать, устанавливать и крепить электронные элементы на печатные платы;
- У34 – проводить монтаж электронных элементов на печатных платах;
- У35 – контролировать качество пайки; производить сборку лицевых панелей приборов;
- У36 – крепить жгуты, кабели и провода к платам и шасси приборов;
- У37 – пользоваться инструментом и приспособлениями для сборки аппаратуры;
- У38 – осуществлять визуальный, электрический и механический контроль монтажа.

знать:

- 31 – принципы построения информационно-телекоммуникационных систем и сетей;
- 32 – базовые технологии построения и состав оборудования мультисервисных сетей связи; 33 – состав и основные характеристики типового оборудования ИТКС; 34 – принципы передачи информации в ИТКС; 35 – принцип модуляции сигналов ИТКС;

- 36 – принципы помехоустойчивого кодирования сигналов ИТКС; 37 – виды и характеристики сигналов в ИТКС;
- 38 – принципы аналого-цифрового преобразования, работы компандера, кодера и декодера; 39 – особенности распространения электромагнитных волн различных диапазонов частот; 310 – виды помех в каналах связи, методы защиты от них; 311 – разновидности проводных линий передачи;
- 312 – конструкцию и характеристики электрических и оптических кабелей связи;
- 313 – способы коммутации в сетях связи;
- 314 – принципы построения многоканальных систем передачи;
- 315 – принципы построения радиолиний и систем радиосвязи;
- 316 – основы маршрутизации в информационно-телекоммуникационных сетях;
- 317 – принципы построения, основные характеристики и оборудование систем подвижной радиосвязи;
- 318 – технологии и оборудование удаленного доступа в информационно-телекоммуникационных сетях;
- 319 – типовые услуги, предоставляемые с использованием информационно-телекоммуникационных сетей, виды информационного обслуживания, предоставляемые пользователям;

- 320 – принципы построения и технические средства локальных сетей;
- 321 – принципы функционирования маршрутизаторов;
- 322 – модемы, используемые в ИТКС, принципы подключения и функционирования;
- 323 – спецификацию изделий, комплектующих, запасного имущества и ремонтных материалов, порядок их учета и хранения;
- 324 – принципы организации эксплуатации ИТКС;
- 325 – содержание технического обслуживания и восстановления работоспособности оборудования ИТКС;
- 326 – принципы организации и технологию ремонта оборудования ИТКС;
- 327 – периодичность проверок контрольно-измерительной аппаратуры;
- 328 – принцип действия выпрямителей переменного тока;
- 329 – принципы работы стабилизаторов напряжения и тока, импульсных источников питания.
- 330 – принципы защиты электронных устройств от недопустимых режимов работы;
- 331 – принципы построения, основные характеристики типовых измерительных приборов и правила работы с ними;
- 332 – основные понятия и определения метрологии, стандартизации и сертификации.
- 333 – методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
- 334 – особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
- 335 – типовые модели управления доступом;
- 336 – типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- 337 – типовые средства и методы ведения аудита и обнаружение вторжений;
- 338 – типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
- 339 – основные понятия криптографии и типовые криптографические методы защиты информации.
- 340 – физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- 341 – номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации;
- 342 – основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам;
- 343 – номенклатуру применяемых средств охраны объектов, систем видеонаблюдения.
- 344 – основные сведения о профессии монтажника радиоэлектронной аппаратуры и приборов;
- 345 – принципы организации рабочего места;
- 346 – основные виды электрорадиоэлементов и конструктивных деталей, марки проводов и кабелей, применяемых при монтаже радиоаппаратуры;
- 347 – основные требования, предъявляемые к электрическому монтажу, установке и креплению навесных электрорадиоэлементов и конструктивных деталей при объемном и печатном монтаже;
- 348 – назначение и применение изоляционных материалов, основных видов припоев и флюсов.

- 349 – способы пайки и предъявляемые к ней требования, особенности пайки полупроводниковых приборов и микросхем;
- 350 – назначение приспособлений, контрольно-измерительных инструментов и приборов, правила пользования ими;
- 351 – строго выполнять мероприятия по охране труда и противопожарной защите при выполнении сборочных и электромонтажных работ;

4. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

4.1. Тематический план программы производственной практики

Коды профессиональных компетенций	Наименования профессиональных модулей	Всего часов	Семестр
1	2	3	4
ПК 1.1 – 1.4	ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей	216	2,3
ПК 2.1. – ПК 2.3.	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	180	4,5
ПК 3.1. – ПК 3.4.	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	72	5,
ПК 1.1– ПК 3.4.	ПМ.04 Освоение одной или нескольких профессий рабочих, должностей служащих	108	6
	<i>Дифференцированный зачет</i>		3,5,6
	Всего:	576	

4.2. Содержание обучения по программе производственной практики

ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей	
<ol style="list-style-type: none"> 1. Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда. 2. Ознакомление с кабельными цехами и участками. 3. Работа с технической документацией. 4. Изучение оборудования и устройств, повышающих работоспособность и надежность кабельных линий. 5. Ознакомление с оборудованием ИТКС. 6. Изучение и работа с контрольно-измерительным оборудованием. 7. Самостоятельная работа на закрепленном рабочем месте. 8. Выполнение индивидуального задания по практике. 9. Участие в аварийных и профилактических работах, проводимых на кабельном участке. 10. Обобщение материала, оформление отчета, сдача зачета. 	216
ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	
<ol style="list-style-type: none"> 1. Участие в организации работ по защите персональных компьютеров на предприятии 2. Участие в организации работ по защите локальных сетей на предприятии 3. Участие в организации работ по защите работ в глобальной сети интернет на предприятии 4. Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. 5. Администрирование систем безопасности проводной защищенной локальной сети. 6. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. 7. Администрирование систем безопасности беспроводной защищенной локальной сети. 8. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. 9. Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей 10. Подключение, установка драйверов, настройка программных средств абонентского шифрования 11. Администрирование внедренных средств 12. Настройка средств электронной подписи 13. Администрирование средств электронной подписи 14. Администрирование средств РКІ 	180
ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	
<ol style="list-style-type: none"> 1. Выполнение подбора, настройки и применения технических средств защиты информации 2. Использование средств охраны и безопасности объекта 3. Организация и реализация технической охраны объектов 	72

<ol style="list-style-type: none"> 4. Выполнение мероприятий по предотвращению несанкционированного доступа к информации 5. Настройка системы защиты информации от съема и утечки по техническим каналам 6. Изучение порядка применения нормативных правовых актов 7. Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами 8. Выявление технических каналов утечки информации 9. Применение существующих способов выявления опасности целостности информации 10. Анализ объектов информатизации предприятий, учреждений, организаций 11. Анализ ресурсов обеспечения инженерно-технической защиты информации 12. Изучение основных этапов проектирования системы защиты информации техническими средствами 13. Проектирование рабочих проектов по системе пожарно-охранной сигнализации, видеонаблюдения, СКУД 14. Оформление технической и технологической документации 	
ПМ.04 Освоение одной или нескольких профессий рабочих, должностей служащих	
<ol style="list-style-type: none"> 1. Обработка и пайка провода без изоляции. 2. Обработка и пайка проводов к лепестковым контактам 3. Обработка и пайка проводов к штырьковым и трубчатым контактам 4. Обработка и пайка экранированных проводов. 5. Установка и пайка радиоэлементов при объемном монтаже 6. Демонтаж объемного монтажа 7. Установка резисторов и конденсаторов на односторонние печатные платы. Пайка 8. Установка и пайка полупроводниковых элементов и микросхем на односторонние печатные платы 9. Различные виды формовки выводов элементов в соответствии с требованиями к монтажу. 10. Установка и пайка радио элементов на двухсторонние печатные платы. 11. Пайка радиоэлементов на макетную плату по схеме. 12. Демонтаж односторонних и двухсторонних печатных плат 13. Создание конструкторской документации 14. Изготовление печатной платы 15. Установка и пайка радиоэлементов 16. Тестирование и настройка устройства 17. Проверка работоспособности устройства 	108

5. Общие требования к организации образовательного процесса

Производственная практика проводится концентрированно после освоения всех разделов модуля. Базами производственной практики являются предприятия и организации, с которыми колледж заключает договор о взаимном сотрудничестве. Основными условиями прохождения производственной практики в данных предприятиях и организациях являются наличие квалифицированного персонала, оснащённость современным оборудованием. Обязательным условием допуска к производственной практике в рамках профессиональных модулей: ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей, ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты, ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, ПМ.04 Освоение одной или нескольких профессий рабочих, должностей служащих.

Практика проводится под руководством преподавателей и специалистов предприятия-базы практики. Руководитель назначается приказом из числа преподавателей специальных дисциплин. В обязанности преподавателя-руководителя практики входит: контроль выполнения программы практики, оказание методической и практической помощи обучающему при отработке практических профессиональных умений и приобретения практического опыта, проверка заполнения дневника по производственной практике.

Руководители практики от предприятия-базы практик назначаются приказом руководителя предприятия до начала практики, из числа специалистов имеющих образование, соответствующее профилю преподаваемого профессионального модуля.

Аттестация по итогам производственной практики проводится на основании результатов, подтверждаемых отчётами и дневниками практики обучающихся, а также отзывами руководителей практики на обучающего.

Производственная практика завершается зачётом обучающего освоенных общих и профессиональных компетенций.

Результаты прохождения производственной практики учитываются при проведении государственной (итоговой) аттестации.

6. Учебно-методическое и информационное обеспечение

Основные источники:

1. Гаврилов, М. В. Информатика и информационные технологии : учебник для СПО / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2018. — 383 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-03051-8. — Режим доступа : www.biblio-online.ru/book/1DC33FDD-8C47-439D-98FD-8D445734B9D9.
2. Галас В.П. Вычислительные системы, сети и телекоммуникации. Часть 2. Сети и телекоммуникации [Электронный ресурс] : электронный учебник / В.П. Галас. — Электрон. текстовые данные. — Владимир: Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, 2016. — 311 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/57364.html>
3. Метрология. Теория измерений : учебник для СПО / В. А. Мещеряков, Е. А. Бадеева, Е. В. Шалобаев ; под общ. ред. Т. И. Мурашкиной. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 167 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-08652-2. — Режим доступа : www.biblio-online.ru/book/8E4273C5-57BF-42FA-AB78-2FBF27037000.
4. Нестеров, С. А. Информационная безопасность : учебник и практикум для СПО / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-07979-1. — Режим доступа : www.biblio-online.ru/book/1997F695-44FF-4570-BF5D-882F5286AE77.

5. Нефедов, В. И. Радиотехнические цепи и сигналы : учебник для СПО / В. И. Нефедов, А. С. Сигов ; под ред. В. И. Нефедова. — М. : Издательство Юрайт, 2018. — 266 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-03409-7. — Режим доступа : www.biblio-online.ru/book/317C5851-EFF0-4AC6-B9DF-F6FC78C228FD.
6. Цветкова М. С. Информатика и ИКТ [Электронный ресурс]: учебник для СПО / М. С. Цветкова, Л.С.Великович - 6-е изд., стер. - М. : ИЦ Академия, 2014. - 352 с. - Режим доступа: <http://www.academia-moscow.ru/reader/?id=81671>
7. Шишмарев В. Ю. Метрология, стандартизация, сертификация и техническое регулирование [Электронный ресурс]: учебник для СПО / В. Ю. Шишмарев - 4-е изд., стер. - М. : ИЦ Академия, 2014. - 320 с. - Режим доступа: <http://www.academia-moscow.ru/reader/?id=336389>
8. Штыков, В. В. Введение в радиоэлектронику : учебник и практикум для СПО / В. В. Штыков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 271 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-03896-5. — Режим доступа : www.biblio-online.ru/book/AA17105C-AD4E-40E4-934E-3C233C357967.

Дополнительные источники:

1. Кузин А. В. Компьютерные сети [Электронный ресурс]: Учебное пособие / Кузин А.В., Кузин Д.А. - 4-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 192 с.: 60x90 1/16. - (Профессиональное образование). - Режим доступа: <http://znanium.com/bookread2.php?book=536468>
2. Басалова Г.В. Основы криптографии [Электронный ресурс] / Г.В. Басалова. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 282 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52158.html>
3. Нетёсова, О. Ю. Информационные технологии в экономике : учебное пособие для СПО / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 178 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-09107-6. — Режим доступа : www.biblio-online.ru/book/4EF2DE26-45A2-4BBD-B0E6-5DF7C448253A.
4. Бурькова Е.В. Физическая защита объектов информатизации [Электронный ресурс] : учебное пособие / Е.В. Бурькова. — Электрон. текстовые данные. — Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2017. — 158 с. — 978-5-7410-1697-8. — Режим доступа: <http://www.iprbookshop.ru/71349.html>
5. Нестеров, С. А. Информационная безопасность : учебник и практикум для СПО / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-07979-1. — Режим доступа : www.biblio-online.ru/book/1997F695-44FF-4570-BF5D-882F5286AE77.
6. Технические средства информатизации: Учебник / Зверева В.П., Назаров А.В. - М.:КУРС, НИЦ ИНФРА-М, 2017. - 256 с.: 60x90 1/16. - (Среднее профессиональное образование) (Переплёт 7БЦ) ISBN 978-5-906818-88-1 - Режим доступа: <http://znanium.com/bookread2.php?book=615331>

Перечень программного обеспечения

Операционная система MS Windows 7 Pro - DreamSpark Premium Electronic Software Delivery (3 years) Renewal по договору - Сублицензионный договор № Tr000074357/КНВ 17 от 01 марта 2016 года

Autodesk Product Design Suite Ultimate 2014-2017 AutoCAD - Электронная лицензия Education Network license Multi-user 3000 concurrent users 3-year term

"MS Visio 2010 - DreamSpark Premium Electronic Software Delivery (3 years) Renewal по договору – Сублицензионный договор № Tr000074357/КНВ 17 от 01 марта 2016 года"

Система защиты информации от несанкционированного доступа Dallas Lock - Договор о сотрудничестве с образовательным учреждением 127-17-153/1

Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-1 - Лицензионный договор № РБТ-14/1607-01-ВУЗ на предоставление права использования программы для ЭВМ

Max Patrol Education - Лицензионный договор № 003-17/ЕМ

XSpider Education - Лицензионный договор № 005-17/ЕХ

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Результаты (освоенные профессиональные и общие компетенции)	Формы и методы контроля и оценки
ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей.	экспертная оценка выполнения практической работы
ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей.	экспертная оценка выполнения практической работы установке программного обеспечения
ПК 1.3. Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей.	Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения
ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.	Наблюдение и экспертная оценка выполнения работ по осуществлению контроля функционирования систем и сетей
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно-телекоммуникационных систем и сетей.	экспертная оценка выполнения практической работы установке программного обеспечения
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения
ПК 2.3. Осуществлять защиту информации от несанкционированных	Наблюдение и экспертная оценка выполнения работ по защите информации от

<p>действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.</p>	<p>несанкционированных действий и специальных воздействий</p>
<p>ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.</p>	<p>экспертная оценка выполнения практической работы по защите информации от утечки по техническим каналам связи</p>
<p>ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.</p>	<p>экспертная оценка выполнения практической работы установке программного обеспечения</p>
<p>ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.</p>	<p>Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения</p>
<p>ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.</p>	<p>Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения</p>
<p>Промежуточная аттестация</p>	<p>Дифференцированный зачет</p>