Федеральное агентство связи
Колледж телекоммуникаций
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Согласовано:
Генеральный директор
Андрианова Светлана Сергеевна
ООО «Аудиторы корпоративной безопасности»
_____ /Андрианова С.С. /
«__» _____ 2020 г.

УТВЕРЖДЕНО
приказом директора КТ МТУСИ
№ 01-03-1137 от «19» июня 2020
_____ С.Н. Ильиных

ПРОГРАММА
УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

по ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

для специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(очная форма обучения)

Москва, 2020 г.

ОДОБРЕНА
предметной (цикловой) комиссией
Компьютерных систем и безопасности
наименование комиссии

Протокол № 5
от «09» июня 2020 г.

Председатель предметной (цикловой) комиссии
_____ / Сергеева М.Б.

Разработано на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (приказ Минобрнауки России № 1551 от 09 декабря 2016 года) и примерной основной образовательной программы 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем. Зарегистрировано в государственном реестре примерных основных образовательных программ № 10.02.04-170703. Реквизиты решения ФУМО о включении ПООП в реестр: Протокол № 1 от 28.03.2017

Рассмотрена и одобрена на заседании методического совета
«10» июня 2020 г. Протокол № 5

СОГЛАСОВАНА:
Заместитель директора по учебно-производственной работе
_____ / С.Г. Алюшина

Организация-разработчик:
КТ МТУСИ, г. Москва

Разработчик:
Преподаватель КТ МТУСИ: Пономарева М.Г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1.1. Область применения программы практики

Программа учебной и производственной практики по ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты является частью образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.2. Место учебной и производственной практики в структуре основной профессиональной образовательной программы: Профессиональный учебный цикл.

1.3. Цели и задачи программы – требования к результатам освоения

Учебная и производственная практики направлены на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках модулей ОПОП СПО по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем**:** квалификация **- техник по защите информации**

Учебная и производственная практики базируются на междисциплинарных курсах профессионального модуля:

МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе, криптографических средств защита

МДК.02.02. Криптографическая защита информации

В результате прохождения практики обучающийся должен:

иметь практический опыт:

монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (далее –ИТКС);

текущего контроля функционирования оборудования ИТКС;

диагностики технического состояния приёмо-передающих устройств и линейных сооружений связи и источников питания;

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

мониторинга технического состояния и работоспособности приёмо-передающих устройств и линейных сооружений связи и источников питания ИТКС;

уметь:

осуществлять техническую эксплуатацию линейных сооружений связи;

производить монтаж кабельных линий и оконечных кабельных устройств;

настраивать, эксплуатировать и обслуживать оборудование ИТКС;

осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС;

производить испытания, проверку и приемку оборудования ИТКС;

производить монтаж кабельных линий и оконечных кабельных устройств ИТКС;

применять средства измерений характеристик функционирования электрических цепей и сигналов ИТКС;

осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС;

осуществлять диагностику технического состояния ИТКС;

проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры;

производить настройку программного обеспечения коммутационного оборудования защищенных телекоммуникационных систем;

производить контроль параметров функционирования ИТКС;

проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС;

осуществлять техническую эксплуатацию приемо-передающих устройств;

оформлять эксплуатационно-техническую документацию;

знать:

принципы построения и основные характеристик ИТКС;

принципы передачи информации в ИТКС;

виды и характеристики сигналов в ИТКС;

виды помех в каналах связи ИТКС и методы защиты от них;

разновидности линий передач, конструкции и характеристики электрических и оптических кабелей связи;

технологии и оборудования удаленного доступа в ИТКС;

принципы построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС;

основные характеристики типовых измерительных приборов и правил работы с ними;

периодичность выполнения поверок контрольно-измерительной аппаратуры;

требования метрологического обеспечения функционирования ИБТКС;

принципы организации технической эксплуатации ИТКС;

спецификацию изделий, комплектующих, запасного имущества и принадлежностей ИТКС.

1.4. Количество часов на освоение программы учебной и производственной практики:

Количество часов практики: всего – 180 часов,

из них

учебная практика – 36 часа,

производственная практика – 144 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРАКТИКИ

2.1. Результатом освоения программы учебной и производственной практики профессионального модуля ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты является овладение профессиональными (ПК) и общими (ОК) компетенциями

Код	Наименование результата обучения
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 оборудование информационно – телекоммуникационных систем и сетей
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и 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 программ-но-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.
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 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Объем учебной и производственной практики

Вид работы	**Объём в часах**
Объем образовательной программы	**180**
в том числе:	
учебная практика	36
производственная практика	144
Промежуточная аттестация: дифференцированный зачет	

3.2. Тематический план и содержание учебной и производственной практики по ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

Наименование разделов и тем	Содержание учебного материала	Объём в часах	Осваиваемые элементы компетенций
1	2	3	4
	Учебная практика		
Раздел 1. Программно-аппаратные средства защиты информации.		**12**	
Тема 1.1. Выбор, подключение, настройка межсетевого экрана.	**Содержание учебного материала**		ПК 2.1. – ПК 2.3. ОК 01 - ОК 04 ОК 09 - ОК 10
	. Классификация сетевых атак. Технологии межсетевых экранов.	2	
	Классификация межсетевых экранов. Топология сети с межсетевым экраном.		
	. Политики межсетевого экрана. Алгоритмы фильтрации.		
Тема 1.2. Администрирование межсетевого экрана	**Содержание учебного материала**		ПК 2.1. – ПК 2.3. ОК 01 - ОК 04 ОК 09 - ОК 10
	Политика межсетевого экрана, основанные на IP-адресах и протоколах. Политики, основанные на идентификации пользователя. Политики, основанные на сетевой активности. Конфигурирование и тестирование межсетевого экрана.	2	
Тема 1.3. Ознакомление, подключение, настройка системы резервного копирования	**Содержание учебного материала**		ПК 2.1. – ПК 2.3. ОК 01 - ОК 04 ОК 09 - ОК 10
	Выбор данных для резервного копирования. Выбор хранилища резервной копии. Репликации хранилища. Правила хранения резервных копий. Планирование резервного копирования. Ежедневное, еженедельное и ежемесячное расписание резервных копий. Правила восстановления объектов из резервных копий.	2	
Тема 1.4. Администрирование системы резервного копирования.	**Содержание учебного материала**		ПК 2.1. – ПК 2.3. ОК 01 - ОК 04 ОК 09 - ОК 10
	Планы и задания резервного копирования. Журнал резервного копирования. Проверка архивов и резервных копий. Операции, доступные в хранилищах.	2	
Тема 1.5. Ознакомление, подключение, настройка системы	**Содержание учебного материала**		ПК 2.1. – ПК 2.3. ОК 01 - ОК 04 ОК 09 - ОК 10
	Классификация и отличительные особенности вредоносных программ. Установка и активация различных антивирусов. Технологии обнаружения вирусов. Сигнатурный и эвристический анализ. Режимы работы антивирусов	2	

антивирусной защиты			
Тема 1.6. Администрирование системы антивирусной защиты.	**Содержание учебного материала**		ПК 2.1. – ПК 2.3. ОК 01 - ОК 04 ОК 09 - ОК 10
	.Карантин подозрительных файлов. Лечение и удаление зараженных файлов. Проверки в режиме реального времени. Проверки по требованию. Восстановление из резервной копии.	2	
Раздел 2. Комплексная система защиты информации.		**24**	
Тема 2.1. Проведение инструктажа по технике безопасности. Составление алгоритма хэш-функции	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Свойства информационной безопасности. Техника безопасности. Криптографическая защита. Метод хэширования. Свойства хэш-функций.	2	
Тема 2.2. Составление алгоритма шифра	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Алгоритм MD5. Алгоритмы SHA. Алгоритмы RIPEMD.	2	
Тема 2.2. Средство шифрования Криптон	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Функциональные возможности средства шифрования Криптон. Программный интерфейс средства шифрования Криптон. Работа шифратора.	2	
Тема 2.3. Подключение, установка драйверов, настройка программных средств шифрования Криптон.	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Инсталляция, настройка модулей программного интерфейса средства шифрования Криптон. Схемы шифрования. Конфигурация драйвера плат шифрования.	2	
Тема 2.4. Администрирование программных средств шифрования Криптон.	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Алгоритм обращения программы к средству шифрования. Уровень приложений. Интерфейс между приложением и драйвером Криптон. Уровень ядра операционной системы. Настройка конфигураций.	2	
Тема 2.5. Подключение,	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04
	Аппаратные средства шифрования. Трехуровневая иерархия ключей. Сеансовые	2	

установка драйверов, настройка аппаратных средств шифрования Криптон.	или пакетные ключи. Долговременные пользовательские или сетевые ключи. Главные ключи. Ячейки памяти шифропроцессора. Этапы шифрования данных. Симметричная и асимметричная криптографические системы.		ОК 09-ОК 10
Тема 2.6. Администрирование аппаратных средств шифрования Криптон.	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Уровень ядра операционной системы. Аппаратный уровень. Хранение внешних носителей ключа. Сеанс шифрования. Дифференцированный зачет	6	
Всего:		**36**	
	Производственная практика		
Раздел 1. Организация информационной безопасности на предприятии.		**144**	
Тема 1.1. Участие в организации работ по защите персональных компьютеров на предприятии	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Защита персональных данных. Политика информационной безопасности на предприятии. Антивирусная защита рабочего места. Поддержка обновлений. Проверка гиперссылок. Политика сложных паролей. Защищенная среда обработки данных. Предотвращение утечек данных. Безопасность приложений.	6	
Тема 1.2. Участие в организации работ по защите локальных сетей на предприятии	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Изучение типов атак и уязвимостей. Средства защиты информации. Топология защищенной сети. Меры и средства обеспечения информационной безопасности.	6	
Тема 1.3. Участие в организации работ по защите работ в глобальной сети интернет на предприятии	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Сегментация сети. Межсетевые экраны. Политики межсетевых экранов. Алгоритмы фильтрации. Аутентификация пользователей. Политика безопасности. Процедурные меры. Виртуальные частные сети. Системы обнаружения вторжений.	6	
Тема 1.4. Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети.	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Сегментация сети. Защищенная среда передачи данных. Средства защиты информации. Разработка системы защиты информации. Безопасность трафика.	6	
Тема 1.5.	**Содержание учебного материала**		ПК 2.1 – ПК 2.3

Администрирование систем безопасности проводной защищенной локальной сети.	Политика безопасности. Управление событиями, данными об информационной безопасности. Управление инцидентами безопасности. Журнал событий. Поведенческая аналитика. Управление доступом.	6	ОК 01-ОК 04 ОК 09-ОК 10
Тема 1.6. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети.			
	Модули безопасности беспроводного доступа. Аутентификация пользователей. Защищенные каналы передачи данных. Безопасность мобильных устройств. Настройка систем безопасности беспроводных защищенных локальных сетей. Шифрование данных.	6	ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
Тема 1.7. Администрирование систем безопасности беспроводной защищенной локальной сети.	**Содержание учебного материала**		
	Политика безопасности. Управление событиями, данными об информационной безопасности. Управление инцидентами безопасности. Журнал событий. Поведенческая аналитика. Управление доступом. Настройка систем шифрования.	6	ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
Тема 1.8. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей.	**Содержание учебного материала**		
	Резервное копирование данных. Правила и расписание резервного копирования. Схемы репликации устройств. Применение средств криптографической защиты. Обновление настроек конфигурации программных и программно-аппаратных средств защиты информации. Обновление политики информационной безопасности.	6	ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
Тема 1.9.	**Содержание учебного материала**		ПК 2.1 – ПК 2.3

Проведение инструктажа по технике безопасности. Ознакомление с предприятием. .	Знакомство с предприятием, изучение техники безопасности на предприятии.	12	ОК 01-ОК 04 ОК 09-ОК 10
Тема 1.10. Выбор программных средств шифрования в соответствии с решаемой задачей.	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Средства шифрования. Классификация средств шифрования. Задачи шифрования. Выбор данных для шифрования. Алгоритмы и методы шифрования данных. Виртуальные частные сети. Защищенная электронная почта. Обеспечение безопасности электронных платежей.	12	
Тема 1.11. Подключение, установка драйверов, настройка программных средств абонентского шифрования	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Программные средства шифрования. Реализуемые криптографические алгоритмы. Ключевая система и ключевые носители. Сетевая аутентификация.	12	
Тема 1.12. Администрирование внедренных средств	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Настройка политик безопасности. Управление событиями, мониторинг трафика, поведенческая аналитика. Обновление настроек конфигураций средств защиты информации.	12	
Тема 1.13. Настройка средств электронной подписи	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Инсталляция. Установка драйверов ключевых носителей. Установка сертификатов. Настройка ключевых контейнеров. Настройка приложений.	18	
Тема 1.14. Администрирование средств электронной	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Управление ключами. Размеры ключей, хранение ключевых носителей. Сроки действия ключей. Уничтожение ключей.	12	

подписи			
Тема 1.15. Администрирование средств PKI	**Содержание учебного материала**		ПК 2.1 – ПК 2.3 ОК 01-ОК 04 ОК 09-ОК 10
	Инфраструктура открытых ключей. Модель доверия. Распределение и отзыв сертификатов. Дифференцированный зачет	18	
Всего:		**144**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ ПРАКТИК

4.1. Для реализации программы учебной практики предусмотрены следующие помещения:

Лаборатория «Программных и программно-аппаратных средств защиты информации» оборудована для проведения занятий лекционного типа, практических занятий, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования, находящегося в кабинете:

Рабочее место преподавателя (стол, стул, персональный компьютер)

- учебная мебель (столы, стулья)
- персональные компьютеры не ниже Core i3
- коммутатор
- интерактивная доска
- проектор
- аппаратно-программные средства обеспечения разграничения и контроля доступа пользователей АПМДЗ "КРИПТОН-ЗАМОК/К" (М-526А) в комплекте со считывателем смарт карт и устройством для подключения iButton

Аппаратный шифратор для PC-совместимых компьютеров «КРИПТОН-8/PCI» в комплекте со считывателем смарт карт и устройством для подключения iButton

- многофункциональный поисковый прибор ST 031 "Пиранья"
- абонентское устройство защиты телефонных линий «Гранит-8»
- устройство защиты аналогового ТА «МП-1А»
- устройство защиты цифрового ТА «МП-1А в евророзетке»
- СИСТЕМНЫЙ КОМПЛЕКТ ARBYTE SILEX M115Q G3/G4400/8GB/4*1TB/RAID
- SATA/k+m/2GLAN/500W/miniTower
- ПАК ViPNet IDS100 2.x
- ПАК ViPNet Coordinator HW50 A 4.x
- Рутокен PINPad
- РУТОКЕН ЭЦП 2.0 память 64 Кбайт
- Рутокен ЭЦП Bluetooth
- Рутокен S 128КБ
- USB-токен JaCarta PKI
- S-Terra

Используемое программное обеспечение:

Контракт № 29ЭА44-2018 от 06.09.2018 (Лицензия на использование JaCarta Management System от 14.09.2018 серийный номер 96d93439-984b-49be-93e0-db5e33051556 бессрочная, Лицензия на использование Secret Disk Server NG для файлового сервера на 10 пользователей (одновременных подключений)(лицензия сервера - E8E3-5990-3795-131C, лицензия администратора 0AEA-7027-899B-36D1) бессрочная, Передача права на использование ПО ViPNet Client for Windows 4.x (КС2)и ПО ViPNet Administrator 4.x (КС2)рег. Номер № 025-00173 от 21.11.2018 – бессрочная., Лицензия на право использования СКЗИ "КриптоПро CSP" версии 4.0 от 30.08.2018 срок неограничен

- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019).

- ОС Microsoft Windows 10 Professional (предустановленное ПО, Контракт № 64ЭА44-2018 от 09.01.2019 с ООО «Азон», бессрочная);

- 7-Zip (свободно распространяемое ПО);

- Mozilla Firefox (свободно распространяемое ПО);

- Foxit Reader (свободно распространяемое ПО);

- Yandex Browser (свободно распространяемое ПО);

- VSCodium (свободно распространяемое ПО);

- Pinta (свободно распространяемое ПО);

- Adobe Reader (свободно распространяемое ПО);

- LibreOffice (свободно распространяемое ПО);

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.)

Учебно-методическая документация

Производственная практика осуществляется на предприятиях г. Москвы и Московской области.

4.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Основная литература

1. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования / Е.Б.Белов, В.Н.Пржегорлинский. - М.: Издательский центр «Академия», 2017. – 336 с.

2. Богомазова Г.Н. Обеспечение информационной безопасности компьютерных сетей: учеб. для студ. учреждений сред. проф. образования / Г.Н.Богомазова. - М.: Издательский центр «Академия», 2017. – 224 с.

3. Рудаков, А.В. Технология разработки программных продуктов[Текст]: учебник для студ. учреждений сред. проф. образования/ А.В. Рудаков. – 11-е изд., стер. – М.: Издательский центр «Академия»,2017. – 208с.

4. Котов, Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов. — Новосибирск : Новосибирский государственный технический университет, 2016. — 59 с. — ISBN 978-5-7782-2959-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91377.html

5. Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : учебное пособие / Ю. А. Котов. — Новосибирск : Новосибирский государственный технический университет, 2017. — 67 с. — ISBN 978-5-7782-3411-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91227.html

Дополнительная литература

1. Майстренко, А. В. Мультимедийные средства обработки информации : учебное пособие для СПО / А. В. Майстренко, Н. В. Майстренко. — Саратов : Профобразование, 2020. — 81 с. — ISBN 978-5-4488-0734-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/90169.html

2. Соловьев, Н. А. Цифровая обработка информации в задачах и примерах : учебное пособие для СПО / Н. А. Соловьев, Н. А. Тишина, Л. А. Юркевская. — Саратов : Профобразование, 2020. — 122 с. — ISBN 978-5-4488-0596-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/92201.html

4.3. Общие требования к организации образовательного процесса

Учебная и производственная практики проводятся при освоении обучающимися профессиональных компетенций в рамках профессионального модуля и реализовываются концентрированно в несколько периодов. Учебная практика проходит в КТ МТУСИ с делением по подгруппам. Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся.

По итогам практики проводится промежуточная аттестация: дифференцированный зачет.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
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 оборудование информационно – телекоммуникационных систем и сетей	- демонстрация знаний типовых программных и программно-аппаратных средств защиты информации в информационно-телекоммуникационных системах и сетях; - демонстрация знаний криптографических средств защиты информации (КСЗИ) конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; - установка и настройка программных и программно-аппаратных, в том числе КСЗИ; - конфигурирование программных и программно-аппаратных, в том числе КСЗИ; - установка, настройка, проведение испытаний и конфигурирование программных и программно-аппаратных, в том числе КСЗИ в оборудовании информационно-телекоммуникационных систем и сетей.	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	- демонстрация знаний порядка тестирования функций программных и программно-аппаратных, в том числе КСЗИ; - демонстрация знаний организации и содержания технического обслуживания и ремонта программно-аппаратных, в том числе КСЗИ; - демонстрация знаний порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные, в том числе КСЗИ. - выявление и оценка угрозы безопасности информации в ИТКС; - поддержание бесперебойной работы программных и программно-аппаратных, в том числе КСЗИ в информационно-телекоммуникационных системах и сетях.	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета
ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных	- демонстрация знаний КСЗИ конфиденциального характера, которые применяются в ИТКС; - демонстрация знаний возможных угроз безопасности информации в ИТКС;	- наблюдение за действиями на практике - оценка действий на

воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программ-но-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	- демонстрация знаний способов защиты информации от НСД и специальных воздействий на нее; - настройка и применение средств защиты информации в операционных системах, в том числе средства антивирусной защиты; - защита информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.	практике - оценка результатов дифференцированного зачета
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	

ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	