Смоленский колледж телекоммуникаций (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

СМОЛЕНСК

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00F35A15D2181C25968B35D1B1F78BE7DA
Владелец: Овчинникова Ирина Александровна
Действителен: с 09.04.2026 до 03.07.2027

УТВЕРЖДАЮ
Зам. директора по учебной работе
_____ И.А. Овчинникова
«14» 05 2025 г.

РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА МДК 02.01 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ

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

среднего профессионального образования

для специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

г. Смоленск, 2025

РАССМОТРЕНО
на заседании методической комиссии
дисциплин сетей связи

Председатель _____ Е.Н.Кожекина
Протокол №14 от «14» 05 2025 г.

СОГЛАСОВАНО
Инженер ООО «Арсенал 67»

_____ Р.Н. Михайлов
«14» 05 2025 г.

СОГЛАСОВАНО
на заседании методической комиссии
информационной безопасности и сетевого
администрирования
Председатель _____ О.Г.Ряска
Протокол №11 от «14» 05 2025 г.

СОГЛАСОВАНО
Методист _____ О.Г. Ряска
«11» 05 2025 г.

Составитель: Королев Е.В. – преподаватель первой квалификационной категории СКТ(ф)СПбГУТ.

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки РФ от 09.12.2016 г. №1551 (ред.03.07.2024),
с учетом примерной основной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, разработанной ФУМО в системе СПО по УГС 10.00.00 «Информационная безопасность».

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

1.1. Область применения программы

Рабочая программа междисциплинарного курса (далее МДК) МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты является частью рабочей программы профессионального модуля ПМ 02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты подготовки специалистов среднего звена в соответствии с ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

1.2. Цели и задачи, требования к результатам освоения МДК

В ходе освоения междисциплинарного курса студент должен овладеть следующими общими и профессиональными компетенциями:

Код	Наименование видов деятельности и компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ВД 2.	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты
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 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.

В результате освоения междисциплинарного курса студент должен:

Иметь практический опыт	в ПО 1- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей; в ПО2 - поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях; в ПО3 - защите 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
уметь	У 1 -выявлять и оценивать угрозы безопасности информации в ИТКС; У 2 -настраивать и применять средства защиты информации в операционных

	системах, в том числе средства антивирусной защиты; У 3 - проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации; У 4- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации; У 5 - проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; У 6-проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; У 7- проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации.
знать	З 1- возможные угрозы безопасности информации в ИТКС; З 2 - способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее; З 3 - типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях; З 5 - порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; З 6 - организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; З 7 - порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации.

Вариативная часть

уметь	У 8 - определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
знать	З 9 - основные протоколы идентификации и аутентификации в телекоммуникационных системах; З 10 - особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;

2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА

2.1 Виды учебной деятельности и количество часов, отводимое на освоение МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

Вид учебной работы	**Объём часов**		
	Обязательная часть	**Вариативная часть**	**Всего**
Максимальная учебная нагрузка (всего)	226	66	**292**
Обязательная аудиторная учебная нагрузка (всего)	226	10	**236**
в том числе:			
теоретическое обучение	130*	10	**140***
практические занятия	30	-	**30**
лабораторные занятия	36	-	**36**
курсовое проектирование (6 семестр)	30	-	**30**
Самостоятельная работа	-	56	**56**
Промежуточная аттестация (5 семестр) - другая форма в форме тестирования			**2***
Промежуточная аттестация (6 семестр) - дифференцированный зачет в форме тестирования			**2***

*Промежуточная аттестация в 5 и 6 семестрах проводится за счет часов лекционной нагрузки

2.2. Тематический план и содержание МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

Разделы	**Код ПК**	**Всего часов (макс. учебная нагрузка и практики)**	**Объём времени**					
			Обязательная аудиторная учебная нагрузка студента, (часов)				Самостоятельная работа студента, часов	
			Всего	В том числе			Всего часов	В том числе
				Лекции	Лаборат. занятия и практич. занятия	Курсовая работа (проект)		Курсовая работа (проект)
	1	***2***	***3***	***4***	***5***	***6***	***7***	***8***
Тема 1.1. Обеспечение безопасности операционных систем	ПК 2.1 - 2.3	62	52	30	12	-	10	-
Тема 1.2. Технологии разграничения доступа	ПК 2.1 - 2.3	60	50	28	22	-	10	-
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	ПК 2.1 - 2.3	60	47	28	14	5	13	-
Тема 1.4. Технологии обнаружения вторжений	ПК 2.1 - 2.3	61	48	30	8	10	13	-
Тема 1.5. Методы управления средствами защиты	ПК 2.1 - 2.3	45	35	20	-	15	10	-
Промежуточная аттестация		4	4	4	-	-	-	-
Консультации		-	-	-	-	-	-	-
Всего		**292**	**236**	**140**	**66**	**30**	**56**	**-**

Наименование разделов междисциплинарного курса (МДК) и тем	Содержание учебного материала, лабораторных и практических занятий, самостоятельной работы обучающихся, курсового проекта	Объем часов	
		Обяз. часть	Вар. часть
1	**2**	**3**	**4**
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			
Тема 1.1. Обеспечение безопасности операционных систем 62 ч	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы.	2	-
	Технологии аутентификации.	2	-
	Аутентификация, авторизация и администрирование действий пользователя.	2	-
	Методы аутентификации	2	-
	Пароли. PIN-коды. Методы надежного составления паролей.	2	-
	Строгая аутентификация.	2	-
	Односторонняя аутентификация.	2	-
	Двухсторонняя аутентификация	2	-
	Аппаратно-программные средства идентификации и аутентификации.	2	-
	Учебный стенд "Системы доверенной загрузки", ПЗИ-МДЗ	2	-
	Настройка программного обеспечения	-	2
	Контроль доступа при запуске ПК	2	-
	Контроль программных и аппаратных средств защищаемой системы	2	-
	Организация защиты от подбора пароля к запускаемой ОС Вести протоколирование доступа к системе	2	-
	Ограничение доступа к файлам и внешним источникам данных	2	-
	Практические занятия	**4**	
	ПЗ 1 Изучение средств идентификации аутентификации операционных систем. Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя.	2	-

	ПЗ 2 Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	2	-
	Лабораторные занятия	**18**	
	ЛЗ 1 Доверенная загрузка ОС.	4	-
	ЛЗ 2 Защита от несанкционированного доступа к ПК.	2	-
	ЛЗ 3 Аутентификация и разграничение доступа пользователей.	2	-
	ЛЗ 4 Механизмы контроля целостности системных файлов.	4	-
	ЛЗ 5 Протоколирование событий доступа к файлам.	2	-
	ЛЗ 6 Контроль печати защищенных документов.	2	-
	ЛЗ 7 Контроль доступа к носителям информации.	2	-
	Самостоятельная работа студентов: составление презентации, подготовка реферата, заполнение рабочей тетради для выполнения практических занятий.	-	**10**
Тема 1.2. Технологии разграничения доступа 60 ч	Функции межсетевых экранов.	2	-
	Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика.	2	-
	Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ.	2	-
	Особенности функционирования межсетевых экранов.	-	2
	Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня.	2	-
	Схемы защиты на базе межсетевых экранов.	2	-
	Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ.	2	-
	Тестирование межсетевых экранов. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.	2	-
	Программные средства защиты информации от несанкционированного доступа	2	-
	Двухфакторную аутентификацию до загрузки системы с помощью аппаратных идентификаторов.	2	-

	Ограничение запуска приложений. Журналирование событий безопасности.	2	-
	Контроль аппаратной и программной целостности системы.	2	-
	Управление пользователями и устройствами системы.	2	-
	Межсетевое экранирование для ограничения доступа к удаленным ресурсам.	2	-
	Практические занятия	**4**	
	ПЗ 3 Архивирование информации	4	-
	Лабораторные занятия	**18**	
	ЛЗ 8 Защищенный вход в систему	4	-
	ЛЗ 9 Ограничение запуска и установки программ	4	-
	ЛЗ 10 Контроль утечки и каналов распространения информации	4	-
	ЛЗ 11 Контроль аппаратной целостности	2	-
	ЛЗ 12 Централизованное управление средствами защиты информации на оконечных устройствах	2	-
	ЛЗ 13 Использование межсетевого экрана для защиты от несанкционированного доступа	2	-
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	-	**10**
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN 55 ч	Проблемы информационной безопасности сетей.	2	-
	Введение в сетевой информационный обмен. Использование сети Интернет.	-	2
	Модель ISO/OSI и стек протоколов TCP/IP.	2	-
	Обеспечение информационной безопасности сетей.	2	-
	Способы обеспечения информационной безопасности.	2	-
	Пути решения проблем защиты информации в сетях.	2	-
	Концепция построения виртуальных защищенных сетей.	2	-
	Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование.	2	-

	VPN – решения для построения защищенных сетей. Виртуальные защищенные сети.	2	-
	Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета.	2	-
	Варианты построения защищенных каналов. Классификация. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP.	2	-
	Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. Защита на сетевом уровне.	2	-
	Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. Организация удаленного доступа. Управление идентификацией и доступом.	2	-
	Средства управления доступом.Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	2	-
	Практические занятия	**14**	
	ПЗ 4 Основные действия с виртуальной машиной	2	-
	ПЗ 5 Работа с контрольными точками	4	-
	ПЗ 6 Использование внешних устройств	4	-
	ПЗ 7 Работа с локальным хранилищем сертификатов в ОС WINDOWS	4	-
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	-	**13**
Тема 1.4. **Технологии обнаружения вторжений** **51 ч**	Технология обнаружения атак.	2	-
	Концепция адаптивного управления безопасностью.	2	-
	Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы.	2	-
	Общие требования к выбираемым средствам анализа защищенности.	2	-
	Средства обнаружения сетевых атак.	2	-

	Методы анализа сетевой информации.	2	-
	Классификация систем обнаружения атак.	2	-
	Компоненты и архитектура системы обнаружения атак.	2	-
	Особенности систем обнаружения атак на сетевом и операционном уровнях.	2	-
	Методы реагирования на сетевые атаки. Обзор современных средств обнаружения атак.	2	-
	Технологии защиты от вирусов.	2	-
	Компьютерные вирусы и проблемы антивирусной защиты.	2	-
	Классификация компьютерных вирусов	2	-
	Жизненный цикл вирусов.	-	2
	Основные каналы распространения вирусов и других вредоносных программ.	2	-
	Практические занятия	**8**	
	ПЗ 8 Изучение средств обнаружения атак	4	-
	ПЗ 9 Изучение антивирусных продуктов	4	-
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	-	**13**
Тема 1.5. **Методы управления средствами защиты** **30 ч**	Методы управления средствами сетевой защиты.	2	-
	Задачи управления системой сетевой защиты.	2	-
	Архитектура управления средствами сетевой защиты.	2	-
	Функционирование системы управления средствами защиты.	2	-
	Аудит безопасности информационной системы.	2	-
	Мониторинг безопасности системы.	2	-
	Программные средства проведения аудита безопасности.	2	-
	Обзор современных систем управления сетевой защитой.	2	-
	Классификация систем защиты.	2	-
	Перспективы и тенденции в развитии систем защиты.	-	2

	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	**-**	**10**
Курсовой проект **Тематика курсовых проектов:** 1. Модель угроз НСД на предприятии 2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии 3. Проведение классификации ПО по требованиям ФСТЭК на предприятии 4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии 5. Построение модели нарушителя по требованиям ФСТЭК на предприятии 6. Построение модели нарушителя по требованиям ФСБ на предприятии 7. Модель угроз безопасности ИС персональных данных на предприятии 8. Комплексная модель защиты информации на предприятии. 9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 13. Проблема защиты информации в облачных хранилищах данных и ЦОДах 14. Защита сред виртуализации.		**30**	**-**
Всего		**222**	**66**
Промежуточная аттестация(5 семестр) - другая форма в виде тестирования		**2**	
Промежуточная аттестация(6 семестр) - дифференцированный зачет в виде тестирования		**2**	
Итого		**292**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МДК 02.01

3.1. Для реализации программы междисциплинарного курса предусмотрены следующие специальное помещение:

Лаборатория программных и программно-аппаратных средств защиты информации (Ауд.315)

Типовой комплект учебного оборудования «Сетевая безопасность» - 1 шт.;

Виртуальный тренажёр «Програмные средства криптографии» - 1 шт.;

Учебно-практический стенд «Системы контроля и управления доступом» – 1 шт.;

Учебный стенд «Программные средства криптографии»– 1 шт.;

Набор программного обеспечения для развёртывания стенда «Программные средства криптографии» - 1 шт.;

Учебный стенд «Системы доверенной загрузки» – 1 шт.;

Учебный стенд «Программные средства защиты информации от несанкционированного доступа» – 1 шт.

Системный блок в комплекте с клавиатурой и мышью: процессор 6 ядер/12 потоков, оперативная память 16 Гб, твердотельный накопитель 1 480 Гб, твердотельный накопитель 2 1000 Гб – 13 шт.;

Локальная сеть с выходом в Интернет топологии «звезда», 1 Гб/сек.

Свободные дистрибутивы операционных систем Linux (Ubuntu, Debian, CentOS).

3.2. Информационное обеспечение реализации программы

ОИ.1 Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714

ОИ.2 Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563

ОИ.3 Маршаков, Д. В. Методы и средства криптографической защиты информации. Практический курс : учебное пособие / Д.В. Маршаков, Д.В. Фахти. — Москва : ИНФРА-М, 2022. — 76 с. — (Высшее образование). - ISBN 978-5-16-110842-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1891129

ОИ.4 Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189341

ОИ5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022

Электронные издания (электронные ресурсы)

Интернет- ресурсы и источники:

1. Электронно-библиотечная система издательства «Лань» [Электронный ресурс]. – Режим доступа: e.lanbook.com
2. Электронно-библиотечная система «Ibooks.ru» [Электронный ресурс]. – Режим доступа: ibooks.ru
3. Электронно-библиотечная система «IPRbook» [Электронный ресурс]. – Режим доступа: iprbookshop.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК 02.01

Код и наименование профессиональных и общих компетенций, 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.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Дифференцированный зачет в форме тестирования Защита отчетов по лабораторным занятиям и практическим занятиям
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации	Дифференцированный зачет в форме тестирования Защита отчетов по лабораторным занятиям и практическим занятиям

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.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Дифференцированный зачет в форме тестирования Защита отчетов по лабораторным занятиям и практическим занятиям

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	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторных занятиях, при выполнении работ практической подготовки по учебной и производственной практикам Экзамен квалификационный
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии 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, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы	
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	

Приложение 1

Лист изменений рабочей программы

Содержание изменения, страница рабочей программы	Дата и номер протокола заседания МК	Основание для внесения изменения
1.		
2.		
3.		
4.		
5.		