Документ подписан квалифицированной электронной подписью
Сертификат: 03489EA30058B4708C45B74E4D79B70F27
Владелец: "АНО ВО ""РОССИЙСКИЙ НОВЫЙ УНИВЕРСИТЕТ"""
Действителен: с 28.05.2026 по 28.08.2027

Автономная некоммерческая организация высшего образования

«Российский новый университет»

(АНО ВО «Российский новый университет»)

Колледж

Рабочие программы учебных дисциплин

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

(очная форма обучения)

на базе основного общего образования

Москва

2026 г.

РАБОЧАЯ ПРОГРАММА

учебной дисциплины
МДК 01.03 СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

для специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем
(базовая подготовка)

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н., _____

Протокол «102/168 от 28.08.2026»

СОДЕРЖАНИЕ

стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ МДК 4

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК 6

3. СТРУКТУРА И СОДЕРЖАНИЕ МДК 7

4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК 21

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК 30

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ
МДК 01.03 СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

1.1. Область применения рабочей программы

Рабочая программа междисциплинарного курса является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения вида деятельности (ВД): Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующих профессиональных компетенций (ПК):

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.2. Цели и задачи МДК – требования к результатам освоения МДК

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

иметь практический опыт:

О1 установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

О2 администрирование автоматизированных систем в защищенном исполнении

О3 эксплуатация компонентов систем защиты информации автоматизированных систем

О4 диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

уметь:

У1 осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем

У2 организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

У3 осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

У4 производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы

У5 настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

У6 обеспечивать работоспособность, обнаруживать и устранять неисправности

знать:

З1 состав и принципы работы автоматизированных систем, операционных систем и сред;

З2 принципы разработки алгоритмов программ, основных приемов программирования;

З3 модели баз данных;

З4 принципы построения, физические основы работы периферийных устройств

З5 теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации

З6 порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях

З7 принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н., «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н., которые актуализируются при изучении междисциплинарного курса:

1) способы защиты информации от утечки по техническим каналам;
2) основные методы управления защитой информации;
3) применять антивирусные средства защиты информации в операционных системах;
4) организационные меры по защите информации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении профессионального модуля:

1) знать и понимать: скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню;
2) знать и понимать: подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;
3) знать и понимать: особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, MWare Workstation;
4) знать и понимать: типы угроз информационной безопасности, типы инцидентов;
5) знать и понимать: Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;
6) знать и понимать: структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;

знать и понимать: подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз

1.3. Планируемые личностные результаты освоения рабочей программы ЛР

2. Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.

ЛР 3. Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.

ЛР 5. Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.

ЛР 6. Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях.

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 8. Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства.

1.4. Количество часов на освоение рабочей программы МДК:

максимальной учебной нагрузки обучающегося – 72 часов, в том числе: аудиторной учебной работы обучающегося – 34 часов, из них в форме практической подготовки – 18 часов; в том числе практических занятий - 20 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК

Результатом освоения МДК является овладение обучающимися видом деятельности - Эксплуатация автоматизированных (информационных) систем в защищенном исполнении в том числе профессиональными компетенциями (ПК):

Код	Наименование результата обучения
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, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных

	(информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

3. СТРУКТУРА И СОДЕРЖАНИЕ МДК

3.1. Объем МДК и виды учебной работы

Вид учебной работы	Объем часов новый
Максимальная учебная нагрузка (всего)	**72**
Аудиторная учебная работа (обязательные учебные занятия) (всего)	**36**
из них в форме практической подготовки	**36**
в том числе:	
теоретические занятия	**18**
лабораторные работы	*
практические занятия	**18**
контрольные работы	*
Самостоятельная работа обучающегося (всего)	*
Консультации	*
Промежуточная аттестация в форме ***дифференцированного зачета***	*

3.2. Тематический план и содержание МДК 01.03 Сети и системы передачи информации

Наименование разделов междисциплинарного курса (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, в том числе в форме практической подготовки, самостоятельная работа обучающихся	Объем часов	Коды личностных результатов, формированию которых способствует элемент программы
1	2	3	
Раздел 1. Теория телекоммуникационных сетей			
Тема 1.1. Основные понятия и определения	Содержание	**4/4**	ОК 01 ОК 03 ПК 1.1 ПК 1.2 ЛР 2 ЛР 3
	1 Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки:	*/*	
	Контрольные работы	*	
Тема 1.2. Принципы передачи информации в сетях и системах связи	Содержание	**2/2**	ОК 05 ПК 1.1 ПК 1.4 ЛР 7 ЛР 8
	1 Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки:	*/*	
	Контрольные работы	*	
Тема 1.3. Типовые каналы передачи и их характеристики	Содержание	**4/4**	ОК 02 ОК 07 ПК 1.1 ПК 1.4 ЛР 6
	1 Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки:	**4/4**	

	Расчет пропускной способности канала связи		
	Контрольные работы	*	
Раздел 2. Сети передачи данных			
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	Содержание	**4/4**	ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 3 ЛР 6
	1 Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи.		
	Протоколы и интерфейсы управления каналами и сетью передачи данных.		
	Лабораторные работы	*	
	Конфигурирование сетевого интерфейса рабочей станции Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне Диагностика и разрешение проблем сетевого уровня Диагностика и разрешение проблем протоколов транспортного уровня Диагностика и разрешение проблем протоколов прикладного уровня	**10/10**	
	Контрольные работы	*	
Тема 2.2. Беспроводные системы передачи данных	Содержание	**2/2**	ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 2 ЛР 5 ЛР 8
	1 Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки: Настройка Wi-Fi маршрутизатора	**4/4**	
	Контрольные работы	*	
Тема 2.3. Сотовые и спутниковые системы	Содержание	**2/2**	ОК 03 ПК 1.2 ЛР 3 ЛР 5
	1 Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки:	*/*	
	Контрольные работы	*	
	Дифференцированный зачет	**2**	

	Консультации	*****	
	Всего:	**36**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК

4.1. Требования к минимальному материально-техническому обеспечению:

Реализация рабочей программы МДК предполагает наличие учебного кабинета лаборатория программных и программно-аппаратных средств защиты информации

Оборудование учебного кабинета:

Комплект учебно-методической документации. Специализированная учебная мебель: стол преподавателя, стул преподавателя, столы для студентов, стулья для студентов, классная доска.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение обучения

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Костров Б. В. Сети и системы передачи информации – М.: Издательский центр «Академия», 2019 -224 с.
2. Организация, принципы построения и функционирования компьютерных сетей: учебник/И.А.Ушаков-М.:Академия,2019-240 с.
3. Интеллектуальные системы : учебник и практикум для среднего профессионального образования / В. Б. Кудрявцев, Э. Э. Гасанов, А. С. Подколзин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 165 с.
4. Сети и телекоммуникации. Маршрутизация в IP-сетях : учебник и практикум для среднего профессионального образования / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 423 с.
5. Компьютерные сети: учебное пособие/ Кузин А.В. – 4-е изд. – М.: ФОРУМ, 2023. – 190 с.

Дополнительные источники:

1. Компьютерные сети 5-е изд., учебное пособие /Новожилов Е.О. – М.:ИЦ Академия,2017 г.

2. Компьютерные сети. Учебное пособие/ Кузин А.В., Кузин Д.А.- М.: Форум,2017 -190 с.

3. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.

4. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии,

5. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2013.

Электронные издания (электронные ресурсы):

Цифровая образовательная среда СПО PROFобразование:

- Васин, Н. Н. Сети и системы передачи информации : методические указания по курсовому проектированию / Н. Н. Васин, М. В. Кузнецов, И. В. Ротенштейн. — Самара : Поволжский государственный университет телекоммуникаций и информатики, 2016. — 58 c. — ISBN 2227-8397. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/73837 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. Пользователей

- Вичугова, А. А. Инструментальные средства разработки компьютерных систем и комплексов : учебное пособие для СПО / А. А. Вичугова. — Саратов : Профобразование, 2017. — 135 c. — ISBN 978-5-4488-0015-3. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/66387 (дата обращения: 04.09.2020). — Режим доступа: для авторизир. Пользователей

Электронно-библиотечная система:

IPR BOOKS - https://www.iprbookshop.ru/106617.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК

Контроль и оценка результатов освоения МДК осуществляется преподавателем в процессе проведения теоретических и практических занятий, дифференцированного зачет

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта и стандарта компетенции Ворлдскиллс	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и	Проявлять знания и умения в проверке технического состояния, проведении	Экспертная оценка в рамках текущего контроля и на практических

текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.

Рабочая программа учебной дисциплины
МДК.01.05 Эксплуатация компьютерных сетей

Специальность : 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Москва 2026

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н., _____
Протокол «102/168 от 28.08.2026»

СОДЕРЖАНИЕ

стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ МДК 4

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК 6

3. СТРУКТУРА И СОДЕРЖАНИЕ МДК 7

4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК 21

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК 30

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ
МДК 01.05 ЭКСПЛУАТАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Область применения рабочей программы

Рабочая программа междисциплинарного курса является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения вида деятельности (ВД): Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующих профессиональных компетенций (ПК):

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.2. Цели и задачи МДК – требования к результатам освоения МДК

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

иметь практический опыт:

О1 установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

О2 администрирование автоматизированных систем в защищенном исполнении

О3 эксплуатация компонентов систем защиты информации автоматизированных систем

О4 диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

уметь:

У1 осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем

У2 организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

У3 осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

У4 производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы

У5 настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

У6 обеспечивать работоспособность, обнаруживать и устранять неисправности

знать:

З1 состав и принципы работы автоматизированных систем, операционных систем и сред;

З2 принципы разработки алгоритмов программ, основных приемов программирования;

З3 модели баз данных;

З4 принципы построения, физические основы работы периферийных устройств

З5 теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации

З6 порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях

З7 принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н.,
«Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н., которые актуализируются при изучении междисциплинарного курса:

1) способы защиты информации от утечки по техническим каналам;
2) основные методы управления защитой информации;
3) применять антивирусные средства защиты информации в операционных системах;
4) организационные меры по защите информации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении профессионального модуля:

1) знать и понимать: скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню;
2) знать и понимать: подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;
3) знать и понимать: особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, MWare Workstation;
4) знать и понимать: типы угроз информационной безопасности, типы инцидентов;
5) знать и понимать: Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;
6) знать и понимать: структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;

знать и понимать: подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз

1.3. Планируемые личностные результаты освоения рабочей программы

ЛР 1. Осознающий себя гражданином и защитником великой страны.

ЛР 2. Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.

ЛР 3. Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 5. Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.

ЛР 6. Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях.

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

1.4. Количество часов на освоение рабочей программы МДК:

максимальной учебной нагрузки обучающегося – 106 часов, в том числе: аудиторной учебной работы обучающегося – 94 часов, из них в форме практической подготовки –106 часов; в том числе практических занятий - 48 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК

Результатом освоения МДК является овладение обучающимися видом деятельности - Эксплуатация автоматизированных (информационных) систем в защищенном исполнении в том числе профессиональными компетенциями (ПК):

Код	Наименование результата обучения
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, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

3. СТРУКТУРА И СОДЕРЖАНИЕ МДК

3.1. Объем МДК и виды учебной работы

Вид учебной работы	Объем часов новый
Максимальная учебная нагрузка (всего)	**126**
Аудиторная учебная работа (обязательные учебные занятия) (всего)	**90**
из них в форме практической подготовки	**106**
в том числе:	
теоретические занятия	**56**
лабораторные работы	*
практические занятия	**40**
контрольные работы	*
Самостоятельная работа обучающегося (всего)	**26**
Консультации	**3,4**
Промежуточная аттестация в форме ***дифференцированного зачета***	*

3.2. Тематический план и содержание МДК 01.05 Эксплуатация компьютерных сетей

Наименование разделов междисциплинарного курса (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, в том числе в форме практической подготовки, самостоятельная работа обучающихся	Объем часов	Коды личностных результатов, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Основы передачи данных в компьютерных сетях			
Тема 1.1. Модели сетевого взаимодействия	Содержание	**4**	ОК 02 ОК 07 ПК 1.1 ПК 1.4 ЛР 1 ЛР 5
	1 Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.		
	2 Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки: Изучение элементов кабельной системы.	**2**	
	Контрольные работы	*	
Тема 1.2. Физический уровень модели OSI	Содержание	**10**	ОК 01 ОК 03 ПК 1.1 ПК 1.2 ЛР 4 ЛР 7
	1 Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.		
	2 Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.		
	3 Оптоволоконные линии связи		
	4 Стандарты кабелей. Электрическая проводка.		
	5 Беспроводная среда передачи.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки: Создание сетевого кабеля на основе неэкранированной витой пары (UTP) Сварка оптического волокна	**2**	

	Контрольные работы		*	
Тема 1.3. Топология компьютерных сетей	Содержание		**2**	ОК 05 ПК 1.1 ПК 1.4 ЛР 5 ЛР 9
	1	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Разработка топологи сети небольшого предприятия Построение одноранговой сети		**2**	
	Контрольные работы		*	
Тема 1.4. Технологии Ethernet	Содержание		**4**	ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 1 ЛР 6
	1	Обзор технологий построения локальных сетей.		
	2	Технология Ethernet. Физический уровень.		
	3	Технология Ethernet. Канальный уровень		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Изучение адресации канального уровня. MAC-адреса.		**2**	
	Контрольные работы		*	
Тема 1.5. Технологии коммутации	Содержание		**2**	ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 1 ЛР 4
	1	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI.		
	2	Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.		
	3	Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети		
	4	Технология PoweroverEthernet		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Создание коммутируемой сети		**2**	
	Контрольные работы		*	
Тема 1.6. Сетевой протокол IPv4	Содержание		**2**	ОК 01 ОК 03
	1	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.		

	2	Маршрутизация пакетов IPv4		ПК 1.1 ПК 1.4 ЛР 2 ЛР 3
	3	Протоколы динамической маршрутизации		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Изучение IP-адресации.		**2**	
	Контрольные работы		*	
Тема 1.7. Скоростные и беспроводные сети	Содержание		**2**	ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 7
	1	Сеть FDDI. Сеть 100VG-AnyLAN Сверхвысокоскоростные сети Беспроводные сети		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Настройка беспроводного сетевого оборудования		**2**	
	Контрольные работы		*	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet				
Тема 2.1. Основы коммутации	Содержание		**4**	ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 4
	1	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах.		
	2	Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Работа с основными командами коммутатора.		**2**	
	Контрольные работы		*	
Тема 2.2. Начальная настройка коммутатора	Содержание		**2**	ОК 05 ПК 1.1 ПК 1.4 ЛР 9
	1	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.		
	2	Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.		

	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы		**4**	
	Контрольные работы		*	
Тема 2.3. Виртуальные локальные сети (VLAN)	Содержание		**4**	ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 4
	1	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.		
	2	Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Настройка VLAN на основе стандарта IEEE 802.1Q Настройка протокола GVRP. Настройка сегментации трафика без использования VLAN Настройка функции Q-in-Q (Double VLAN). Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.		**4**	
	Контрольные работы		*	
Тема 2.4. Функции повышения надежности и производительности	Содержание		**4**	ОК 05 ПК 1.1 ПК 1.4 ЛР 1 ЛР 2
	1	Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.		
	2	Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.		
	Дополнительные функции защиты от петель. Агрегирование каналов связи.			
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Настройка протоколов связующего дерева STP, RSTP, MSTP. Настройка функции защиты от образования петель LoopBackDetection Агрегирование каналов.		**4**	
	Контрольные работы		*	
Тема 2.5. Адресация сетевого уровня и маршрутизация	Содержание		**2**	ОК 01 ОК 03
	1	Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.		

	2	Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.		ПК 1.1 ПК 1.2 ЛР 1 ЛР 5
	3	Планирование подсетей IPv6. Протокол NDP.		
	4	Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Основные конфигурации маршрутизатора. Расширенные конфигурации маршрутизатора. Работа с протоколом CDP. Работа с протоколом TELNET. Работа с протоколом TFTP. Работа с протоколом RIP. Работа с протоколом OSPF. Конфигурирование функции маршрутизатора NAT/PAT. Конфигурирование PPP и CHAP.		**4**	
	Контрольные работы		*	
Тема 2.6. Качество обслуживания (QoS)	Содержание		**4**	ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 6 ЛР 7
	1	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.		
	2	Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Настройка QoS. Приоритизация трафика. Управление полосой пропускания		**2**	
	Контрольные работы		*	
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	Содержание		**4**	ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 1
	1	Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.		
	2	Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки:		**2**	

	Списки управления доступом (AccessControlList) Контроль над подключением узлов к портам коммутатора. Функция PortSecurity. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding		
	Контрольные работы	*	
Тема 2.8. Многоадресная рассылка	Содержание	**4**	ОК 03 ПК 1.2 ЛР 5 ЛР 7
	1 Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.		
	2 Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping).Функция IGMP FastLeave.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки: Отслеживание трафика многоадресной рассылки. Отслеживание трафика Multicast	**2**	
	Контрольные работы	*	
Тема 2.9. Функции управления коммутаторами	Содержание		ОК 05 ПК 1.1 ПК 1.4 ЛР 1 ЛР 7
	1 Управление множеством коммутаторов. Протокол SNMP.		
	2 RMON (Remote Monitoring). Функция Port Mirroring.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки: Функции анализа сетевого трафика. Настройка протокола управления топологией сети LLDP.	**2**	
	Контрольные работы	*	
Раздел 3. Межсетевые экраны			
Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	Содержание	**2**	ОК 03 ПК 1.2 ЛР 4
	1 Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.		
	2 Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки:	*	
	Контрольные работы	*	

Тема 3.2. Межсетевые экраны	Содержание		**2/2**	ОК 02 ОК 07 ПК 1.1 ПК 1.4 ЛР 1 ЛР 7
	1	Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.		
	2	Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Основы администрирования межсетевого экрана Соединение двух локальных сетей межсетевыми экранами Создание политики без проверки состояния. Создание политик для традиционного (или исходящего) NAT. Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing		**4/4**	
	Контрольные работы		*	
Тема 3.3. Системы обнаружения и предотвращения проникновений	Содержание		**2/2**	ОК 05 ПК 1.1 ПК 1.4 ЛР 6
	1	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.		
	2	Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Обнаружение и предотвращение вторжений.		**2/2**	
	Контрольные работы		*	
Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	Содержание		**2/2**	ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 1 ЛР 5
	1	Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Создание альтернативных маршрутов с использованием статической маршрутизации		**2/2**	
	Контрольные работы		*	
	Дифференцированный зачет		*	

	Консультации	**3,4**	
	Всего:	**126**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК

4.1. Требования к минимальному материально-техническому обеспечению:

Реализация рабочей программы МДК предполагает наличие учебного кабинета лаборатория программных и программно-аппаратных средств защиты информации

Оборудование учебного кабинета:

Комплект учебно-методической документации. Специализированная учебная мебель: стол преподавателя, стул преподавателя, столы для студентов, стулья для студентов, классная доска.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение обучения

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Компьютерные сети: учебное пособие/ Кузин А.В. – 4-е изд. – М.: ФОРУМ, 2023. – 190 с.
2. Организация, принципы построения и функционирования компьютерных сетей: учебник/И.А.Ушаков-М.:Академия,2019-240 с.
3. Костров Б. В. Сети и системы передачи информации – М.: Издательский центр «Академия», 2019 -224 с.

Дополнительные источники:

1. Компьютерные сети 5-е изд., учебное пособие /Новожилов Е.О. – М.:ИЦ Академия,2017 г.
2. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2015.
3. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2013.
4. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

5. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2013.

Электронные издания (электронные ресурсы):

Цифровая образовательная среда СПО PROFобразование:

- Демидов, Л. Н. Основы эксплуатации компьютерных сетей : учебник для бакалавриата / Л. Н. Демидов. — Москва : Прометей, 2019. — 798 с. — ISBN 978-5-907100-01-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/94481 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. Пользователей

- Оливер, Ибе Компьютерные сети и службы удаленного доступа / Ибе Оливер ; перевод И. В. Синицын. — 2-е изд. — Саратов : Профобразование, 2019. — 335 c. — ISBN 978-5-4488-0054-2. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87999 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК

Контроль и оценка результатов освоения МДК осуществляется преподавателем в процессе проведения теоретических и практических занятий, дифференцированного зачет

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта и стандарта компетенции Ворлдскиллс	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и	Проявлять знания и умения в проверке технического состояния, проведении	Экспертная оценка в рамках текущего контроля и на практических

текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.

Рабочая программа учебной дисциплины

МДК 02.02. Криптографические средства защиты информации

Специальность: 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н., _____
Протокол «102/168 от 28.08.2026»

1.ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

МДК 02.02 Криптографические средства защиты информации

1.1. Область применения рабочей программы междисциплинарного курса

Рабочая программа является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения вида деятельности (ВД). Защита информации в автоматизированных системах программными и программно-аппаратными средствами(ПК).

ПК 2.1.Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно- аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.2. Цели и задачи МДК – требования к результатам освоения МДК

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

уметь:

У.1 устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации;

У.2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

У.3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

У.4 применять программные и программно-аппаратные средства для защиты информации в базах данных;

У.5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

У.6 применять математический аппарат для выполнения криптографических преобразований;

У.7 использовать типовые программные криптографические средства, в том числе электронную подпись;

У.8 применять средства гарантированного уничтожения информации;

У.9 устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации;

У.10 осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

знать:

З.1 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

З.2 методы тестирования функций отдельных программных и программно- аппаратных средств защиты информации;

З.3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

З.4 основные понятия криптографии и типовых криптографических методов и средств защиты информации;

З.5 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

З.6 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

1.3. Планируемые личностные результаты освоения рабочей программы

ЛР 1. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»

ЛР 2. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 3. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 4. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 5. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Вид учебной работы	**Объём часов**
Максимальная учебная нагрузка (всего)	252
Обязательная аудиторная учебная нагрузка (всего)	108
в том числе:	
Лекционные занятия (Лек)	98
Практические занятия (Пр)	78
Текущие консультации (ТКонс)	5.1
Самостоятельная работа обучающегося (всего)	70
Внеаудиторная самостоятельная работа	

Распределение учебного времени по темам и видам учебных занятий очная форма обучения

№	Наименование разделов, тем учебных занятий	Всего часов	Контактная работа с преподавателем					Сам. раб.	Формируемые результаты обучения
			Всего	Л	Пр	З	Тконс		
Раздел 1. Математические основы криптографии									
1	Тема 1.1. Математические основы криптографии	26		4	4			7	
Раздел 2. Классическая криптография									
	Тема 2.1. Методы криптографического защиты информации	24		4	4			7	
	Тема 2.2. Криптоанализ	24		4	4			7	
	Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	12		4	4			7	
Раздел 3. Современная криптография									
	Тема 3.1. Кодирование информации. Компьютеризация шифрования	30		6	6			7	
	Тема 3.2. Симметричные системы шифрования	16		4	4			7	
	Тема 3.3. Асимметричные системы шифрования	16		4	4			7	
	Тема 3.4. Аутентификация данных. Электронная подпись	30		6	6			7	
	Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	16		4					
	Тема 3.6. Криптозащита информации в сетях передачи данных	14		4				7	
	Тема 3.7. Защита информации в электронных платежных системах	30		6				7	

	Тема 3.8. Компьютерная стеганография	14		4					
	Промежуточная аттестация						5.1		

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ)

Раздел 1. Математические основы криптографии
Тема 1.1. Математические основы криптографии

1. Предмет и задачи криптографии. История криптографии. Основные термины
2. Элементы теории множеств. Группы, кольца, поля.
3. Делимость чисел. Признаки делимости. Простые и составные числа.
4. Основная теорема арифметики. Наибольший общий делитель. Взаимно
5. простые числа. Алгоритм Евклида для нахождения НОД.
6. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.
7. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.
8. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.
9. Китайская теорема об остатках.
10. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.
11. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.
12. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра
13. Арифметические операции над большими числами.

Раздел 2. Классическая криптография
Тема 2.1. Методы криптографического защиты информации

1. Классификация основных методов криптографической защиты. Методы симметричного шифрования
2. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр
3. Методы перестановки. Табличная перестановка, маршрутная перестановка
4. Гаммирование. Гаммирование с конечной и бесконечной гаммами
Практические занятия, в том числе в форме практической подготовки
1. Применение классических шифров замены
2. Применение классических шифров перестановки
3. Применение метода гаммирования

Тема 2.2. Криптоанализ

1. Основные методы криптоанализа. Криптографические атаки.

2. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса
3. Перспективные направления криптоанализа, квантовый криптоанализ.
Практические занятия, в том числе в форме практической подготовки
1. Криптоанализ шифра простой замены методом анализа частотности символов
2. Криптоанализ классических шифров методом полного перебора ключей
3. Криптоанализ шифра Вижинера
4. Криптоанализ шифра Вижинера

Тема 2.3. Поточные шифры и генераторы псевдослучайных

1. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии
2. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS
Практические занятия, в том числе в форме практической подготовки
1. Применение методов генерации ПСЧ

Раздел 3. Современная криптография
Тема 3.1. Кодирование информации. Компьютеризация шифрования.

1. Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования.
2. Представление информации в двоичном коде. Таблица ASCII. Компьютеризация шифрования. Аппаратное и программное шифрование
3. Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств
Практические занятия, в том числе в форме практической подготовки
1. Кодирование информации
2. Программная реализация классических шифров
3. Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.

Тема 3.2. Симметричные системы шифрования

1. Общие сведения. Структурная схема симметричных криптографических систем
2. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4

Тема 3.3. Асимметричные системы шифрования

1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.
2. Элементы теории чисел в криптографии с открытым ключом.
Практические занятия, в том числе в форме практической подготовки
1. Применение различных асимметричных алгоритмов.
2. Изучение программной реализации асимметричного алгоритма RSA

Тема 3.4. Аутентификация данных. Электронная подпись

1. Аутентификация данных. Общие понятия. ЭП. MAC.
2. Однонаправленные хеш-функции. Алгоритмы цифровой подписи
Практические занятия, в том числе в форме практической подготовки
1. Применение различных функций хеширования, анализ особенностей хешей
2. Применение криптографических атак на хеш-функции.
3. Изучение программно-аппаратных средств, реализующих основные функции ЭП

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации

1. Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. аутентификация
2. Взаимная аутентификация. Односторонняя
Практические занятия, в том числе в форме практической подготовки
1. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.
2. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

Тема 3.6. Криптозащита информации в сетях передачи данных

1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр
2. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.

Тема 3.7. Защита информации в электронных платежных системах

1. Принципы функционирования электронных платежных систем.
2. Электронные пластиковые карты. Персональный идентификационный номер
3. Применение криптографических протоколов для обеспечения безопасности
электронной коммерции.

Тема 3.8. Компьютерная стеганография

1. Скрытая передача информации в компьютерных системах.
2. Проблема аутентификации мультимедийной информации. Защита авторских прав.
3. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ
Практические занятия, в том числе в форме практической подготовки
1. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ
2. Реализация простейших стеганографических алгоритмов

ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Основное оборудование: стенд «Требования к результатам освоения профессиональной образовательной программы , «Компьютер и здоровье», «Области использования вычислительной техники», комплект учебно-методической документации, комплект учебников по количеству обучающихся.

Демонстрационные средства обучения: тематические папки дидактических материалов.

Программное обеспечение общего и профессионального назначения.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

Информационное обеспечение обучения

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК

Контроль и оценка результатов освоения МДК осуществляется преподавателем в процессе проведения теоретических и практических

занятий.

Результаты **(освоенные профессиональные компетенции) с учетом личностных результатов и стандартов**	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением
		различных видов работ

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ

ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с

2. Программно-аппаратные средства защиты информации.

Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.

Дополнительные источники:

1. Белов В.В. Проектирование информационных систем: учебник для студ. учреждений высш. проф. образования / В. В. Белов, В. И. Чистякова; под ред. В. В. Белова – М.: Издательский центр «Академия», 2013.

2. Гвоздева В.А., Лаврентьева И.Ю., Основы построения автоматизированных информационных систем, Москва, ИД Форум – ИНФРА-М, 2009.

3. Гвоздева Т.В., Баллод Б.А., Проектирование информационных систем: учеб.пособие / Т.В. Гвоздева, Б.А. Баллод. – Ростов н/Д: Феникс, 2009. – 508 с.

4. Емельянова Н.З., Устройство и функционирование информационных систем: учеб.пособие для СПО / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – 2-е изд., перераб. и доп. – М.: Форум, 2015. – 448 с.

5. Избачков Ю.С., Информационные системы: учебник для вузов [Гриф УМО МО РФ]. 3-е изд. / Избачков Ю.С., Петров В.Н [и др.]. – СПб.: Питер, 2011. – 544 с.

Электронные издания (электронные ресурсы):

Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 https://e.lanbook.com/book/82817

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. https://urait.ru/bcode/449548

2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. https://urait.ru/bcode/456793

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2020. — 325 с. https://urait.ru/bcode/451933

Цифровая образовательная среда СПО PROFобразование:

- Абрамов, Г. В. Проектирование и разработка информационных систем :

учебное пособие для СПО / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. — Саратов : Профобразование, 2020. — 169 c. — ISBN 978-5-4488-0730-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/88888 (дата обращения: 07.09.2020). — Режим доступа: для авторизир. пользователей.

Рабочая программа учебной дисциплины

МДК.01.01 Операционные системы

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н., _____

Протокол «102/168 от 28.08.2026»

1. НАИМЕНОВАНИЕ И ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы

Рабочая программа междисциплинарного курса является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения вида деятельности (ВД): Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующих профессиональных компетенций (ПК):

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.2. Цели и задачи МДК – требования к результатам освоения МДК

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

иметь практический опыт:

О1 установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

О2 администрирование автоматизированных систем в защищенном исполнении

О3 эксплуатация компонентов систем защиты информации автоматизированных систем

О4 диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

уметь:

У1 осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем

У2 организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

У3 осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

У4 производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы

У5 настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

У6 обеспечивать работоспособность, обнаруживать и устранять неисправности

знать:

З1 состав и принципы работы автоматизированных систем, операционных систем и сред;

З2 принципы разработки алгоритмов программ, основных приемов программирования;

З3 модели баз данных;

З4 принципы построения, физические основы работы периферийных устройств

З5 теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации

З6 порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях

З7 принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н.,

2. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Вид учебной работы	**Объём часов**
Максимальная учебная нагрузка (всего)	72
Обязательная аудиторная учебная нагрузка (всего)	58
в том числе:	
Лекционные занятия (Лек)	28
Практические занятия (Пр)	28
Часы на контрольные работы (КоР)	0,3
Текущие консультации (ТКонс)	1,7
Самостоятельная работа обучающегося (всего)	14
Внеаудиторная самостоятельная работа	

Распределение учебного времени по темам и видам учебных занятий

очная форма обучения

№	Наименование разделов тем	Всего часов	Контактная работа с преподавателем					Сам. раб.	Формируемые результаты обучения
			Всего	Л	Пр	КоР	Тконс		
Раздел 1. Элементы теории операционных систем. Свойства операционных систем									
	Тема 1.1. Основы теории операционных систем	**4**	**4**	**2**	**2**				
	Тема 1.2. Машино зависимые и машинно-независимые свойства операционных систем	**4**	**4**	**2**	**2**			**2**	
	Тема 1.3. Модульная структура операционных систем, пространство пользователя	**4**	**4**	**2**	**2**			**2**	
	Тема 1.4. Управление памятью	**4**		**2**	**2**				
	Тема 1.5. Управление процессами, многопроцессорные системы	**4**	**4**					**2**	
	Тема 1.6. Виртуализация и облачные технологии	**4**	**4**	**2**	**2**			**2**	

Раздел 2. Безопасность операционных систем									
	Тема 2.1. Принципы построения защиты информации в операционных системах	**30**	**30**	**12**	**12**			**4**	
Раздел 3. Особенности работы в современных операционных системах									
	Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	**4**	**4**					**2**	
	Тема 3.2. Операционная система Windows	**12**	**12**	**6**	**6**				
	Тема 3.3. Серверные операционные системы	**2**	**2**						

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК

3.1. Требования к минимальному материально-техническому обеспечению:

Реализация рабочей программы МДК предполагает наличие учебного кабинета лаборатория программных и программно-аппаратных средств защиты информации

Оборудование учебного кабинета:

Комплект учебно-методической документации. Специализированная учебная мебель: стол преподавателя, стул преподавателя, столы для студентов, стулья для студентов, классная доска.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

3.2. Информационное обеспечение обучения

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Операционные системы : учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 164 с.

2. Операционные системы и среды учебник для среднего профессионального образования /Батаев А.В. – 6-е изд., стер. – М.: ОИЦ Академия, 2023.- 288 с.

Дополнительные источники:

1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2014.

2. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.

3. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2013.

Электронные издания (электронные ресурсы):

Цифровая образовательная среда СПО PROFобразование:

Коньков, К. А. Основы операционных систем : учебник для СПО / К. А. Коньков, В. Е. Карпов. — Саратов : Профобразование, 2021. — 346 с. — ISBN 978-5-4488-1003-9. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL:

https://profspo.ru/books/102196 (дата обращения: 22.03.2021). — Режим доступа: для авторизир. Пользователей

Назаров, С. В. Современные операционные системы : учебное пособие / С. В. Назаров, А. И. Широков. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 351 с. — ISBN 978-5-4497-0385-9. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/89474 (дата обращения: 18.11.2020).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК

Контроль и оценка результатов освоения МДК осуществляется преподавателем в процессе проведения теоретических и практических занятий, дифференцированного зачет

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и	Проявлять знания и умения в проверке технического состояния, проведении	Экспертная оценка в рамках текущего контроля и на практических

текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Дифференцированный зачет.

Рабочая программа учебной дисциплины

МДК.02.01 Программные и программно-аппаратные средства обеспечения информационной безопасности

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н., _____
Протокол «102/168 от 28.08.2026»

СОДЕРЖАНИЕ

1. Паспорт программы учебной дисциплины
2. Структура и содержание дисциплины
3. Условия реализации дисциплины
4. Контроль и оценка результатов освоения дисциплины

ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
МДК.02.01 Программные и программно-аппаратные средства обеспечения информационной безопасности

1.1. Место дисциплины в структуре образовательной программы

Учебная дисциплина МДК. 02.01 Программные и программно-аппаратные средства обеспечения информационной безопасности относится к профессиональному модулю ПМ.02 «Защита информации в автоматизированных системах программами и программно-аппаратными средствами» профессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Дисциплина реализуется в традиционном формате, с использованием интерактивных форм проведения учебных занятий, в синхронном и асинхронном режиме на образовательной платформе Юрайт - https://urait.ru/

1.2 Цель и планируемые результаты освоения дисциплины

Содержание программы учебной дисциплины МДК. 02.01 Программные и программно-аппаратные средства обеспечения информационной безопасности направлено на достижение следующей цели - формирование знаний и умений по защите компьютерной информации с применением современных программно-аппаратных средств.

Результатом освоения программы является овладение обучающимися общими (ОК) и профессиональными (ПК) компетенциями, личностными результатами (ЛР):

Общие компетенции

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 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

Профессиональные компетенции

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

Личностные результаты:

ЛР 1. Осознающий себя гражданином России и защитником Отечества, выражающий свою российскую идентичность в поликультурном и многоконфессиональном российском обществе и современном мировом сообществе. Сознающий свое единство с народом России, с Российским государством, демонстрирующий ответственность за развитие страны. Проявляющий готовность к защите Родины, способный аргументированно отстаивать суверенитет и достоинство народа России, сохранять и защищать историческую правду о Российском государстве.

ЛР 2. Проявляющий активную гражданскую позицию на основе уважения закона и правопорядка, прав и свобод сограждан, уважения к историческому и культурному наследию России. Осознанно и деятельно выражающий неприятие дискриминации в обществе по социальным, национальным, религиозным признакам; экстремизма, терроризма, коррупции, антигосударственной деятельности. Обладающий опытом гражданской социально значимой деятельности (в студенческом самоуправлении, добровольчестве, экологических, природоохранных, военно-патриотических и др. объединениях, акциях, программах). Принимающий роль избирателя и участника общественных отношений, связанных с взаимодействием с народными избранниками.

ЛР 4. Проявляющий и демонстрирующий уважение к труду человека, осознающий ценность собственного труда и труда других людей. Экономически активный, ориентированный на осознанный выбор сферы профессиональной деятельности с учетом личных жизненных планов, потребностей своей семьи, российского общества.Выражающий осознанную готовность к получению профессионального образования, к непрерывному образованию в течение жизни Демонстрирующий позитивное отношение к регулированию трудовых отношений. Ориентированный на самообразование и профессиональную переподготовку в условиях смены технологического уклада и сопутствующих социальных перемен. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 6. Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации.

ЛР 7. Осознающий и деятельно выражающий приоритетную ценность каждой человеческой жизни, уважающий достоинство личности каждого человека, собственную и чужую уникальность, свободу мировоззренческого выбора, самоопределения. Проявляющий бережливое и чуткое отношение к религиозной принадлежности каждого человека, предупредительный в отношении выражения прав и законных интересов других людей.

ЛР 9. Сознающий ценность жизни, здоровья и безопасности. Соблюдающий и пропагандирующий здоровый образ жизни (здоровое питание, соблюдение гигиены, режим занятий и отдыха, физическая активность), демонстрирующий стремление к физическому совершенствованию. Проявляющий сознательное и обоснованное неприятие вредных привычек и опасных наклонностей (курение, употребление алкоголя, наркотиков, психоактивных веществ, азартных игр, любых форм зависимостей), деструктивного поведения в обществе, в том числе в цифровой среде.

ЛР 13. Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности.

ЛР 14. Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.

ЛР 15.Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем.

ЛР 16. Соответствующий ожиданиям работодателей: креативно мыслящий, эффективно сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, распределяющий время и другие ресурсы для выполнения поставленной задачи в установленный срок, ответственный, дисциплинированный, целеустремленный, стрессоустойчивый.

ЛР 17. Демонстрирующий культуру речи, в том числе в деловой переписке/переговорах, способный презентовать себя и продукт профессиональной деятельности.

ЛР 18. Демонстрирующий способность использовать в цифровой среде различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.

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

Уметь:

- применять программно-аппаратные средства обеспечения информационной безопасности;
- диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
- оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
- участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
- применять нормативно-правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами;
- использовать криптографические средства и методы защиты информации.

Знать:

- базовый понятийный аппарат в области информационной безопасности;
- функционирование системы управления средствами безопасности;
- основные типы моделей управления доступом;
- методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
- особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, баз данных;
- типовые средства и методы обеспечения информационной безопасности локальных и глобальных вычислительных сетях.

2.СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Объем часов*
Максимальная учебная нагрузка (всего)	*270*
Обязательная аудиторная учебная нагрузка(всего)	*126*
в том числе:	
лекции	*92*
практические занятия	*90*
консультация	*5,1*
Самостоятельная работа обучающегося (всего)	*64*
Промежуточная аттестация в форме итоговой работы	

2.2.Тематический план и содержание дисциплины МДК. 02.01 Программные и программно-аппаратные средства обеспечения информационной безопасности

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
1	2	3	4
Тема 1. Введение в теорию и практику защиты программного обеспечения	**Лекция** Проблема защиты программного обеспечения информационных систем. Объекты защиты. Уязвимости и угрозы безопасности программного обеспечения. Жизненный цикл программного обеспечения информационных систем. Технологическая и эксплуатационная безопасность программного обеспечения. Основные принципы обеспечения безопасности программного обеспечения. Защита программного обеспечения как система научных дисциплин	20	
	Практическое занятие Решение разноуровневых заданий (задач): 1)Задания 1-10, с. 32. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 32 — URL: https://urait.ru/bcode/543631/p.32 2) Задания 1-14, с. 37. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. —	24	Устный (письменный) опрос, оценка навыка анализа и решения профессиональных задач

	(Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 37 — URL: https://urait.ru/bcode/542339/p.37		
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — С. 12 — 32 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543631/p.12-32 **Интерактивные формирующие тесты:** 1. https://urait.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-543631#page/32 - Введение в теорию и практику защиты программного обеспечения 2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 37 — URL: https://urait.ru/bcode/542339/p.37 **Интерактивные формирующие тесты:** 2. https://urait.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-542339#page/37 - Введение в надежность и безопасность программного обеспечения	4	Устный (письменный) опрос тестирование
Тема 2. Основания теории и практики защиты программного обеспечения.	**Лекция** Элементы теории алгоритмов. Элементы теории сложности вычислений. Классы сложности вычислений. Односторонние функции и функции с секретом. Псевдослучайные генераторы. Элементы криптологии. Основные задачи криптографии. Криптосистемы с секретным и открытым ключом. Схемы электронной подписи. Криптографические стойкие схемы хэширования. Криптографические стойкие псевдослучайные генераторы. Схемы вероятностного шифрования. Информационные технологии и операционные системы	20	

	Практическое занятие Решение разноуровневых заданий (задач): 1)Задания 1-15, с. 51 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 51 — URL: https://urait.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-543631#page/51 2) Задания 1-14, с. 153 Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2021. — 259 с. — (Профессиональное образование). — ISBN 978- 5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 153 — URL: https://urait.ru/bcode/543873/p.153 3) Задания 1-3, с. 172 Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2021. — 259 с. — (Профессиональное образование). — ISBN 978- 5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 172 — URL: https://urait.ru/bcode/543873/p.172 4) задания 1-3, с. 178 Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2021. — 259 с. — (Профессиональное образование). — ISBN 978- 5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 178 — URL: https://urait.ru/bcode/543873/p.178	14	Устный (письменный) опрос, оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — С. 33 — 51 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543631/p.33-51 **Интерактивные формирующие тесты:** 1. https://urait.ru/viewer/programmno-apparatnye-sredstva-	4	Устный (письменный) опрос тестирование

	zaschity-informacii-zaschita-programmnogo-obespecheniya-543631#page/51 - Основания теории и практики защиты программного обеспечения Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 51 — URL: https://urait.ru/bcode/543631/p.51 **Интерактивные формирующие тесты:** 2. https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/172 - Современные криптографические алгоритмы Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2021. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 172 — URL: https://urait.ru/bcode/543873/p.172		
Тема 3. Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения	**Лекция** Классификация вредоносных программ. Троянские программы. Компьютерные вирусы. Прочие вредоносные программы. Защита от вредоносных программ. Методы тестирования программного обеспечения на его защищенность. Фаззинг программ. Методы защиты программ от несанкционированного исследования. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. Манипуляции с кодом программы. Методы противодействия динамическим способам снятия защиты программ от копирования. Методы описания и обнаружения уязвимостей программного обеспечения на примере операционных систем Уязвимости на примере ОС Windows Методы обнаружения уязвимостей операционных систем. Подходы к разработке защищенных операционных систем.	16	

	Практическое занятие **Приложение 3.Практическое занятие №1, с. 200:** Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 200 — URL: https://urait.ru/bcode/543631/p.200 Решение разноуровневых заданий (задач): 1)Задания 1-10, с. 97 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 97 — URL: https://urait.ru/bcode/543631/p.97 2)Задания 1-7, с. 47 Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 47 — URL: https://urait.ru/bcode/542339/p.47	20	Устный (письменный) опрос, оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — С. 52 — 97 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543631/p.52-97 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-543631#page/97 - Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения	8	Устный (письменный) опрос тестирование

	2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 47 — URL: https://urait.ru/bcode/542339/p.47 **Интерактивные формирующие тесты** https://urait.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-542339#page/47 - Угрозы надежности и безопасности программного обеспечения		
Тема 4. Средства, системы и комплексы защиты программного обеспечения	**Лекция** Средства и комплексы защиты от вредоносных программ. Средства, системы и комплексы тестирования программного обеспечения при испытаниях его на технологическую безопасность. Методологические основы оценки качества, проведения испытаний и сертификации программных средств. Построение программно-аппаратных комплексов для контроля технологической безопасности программ. Фаззеры программ. Пример тестирования ПО средств защиты информации. Обфускаторы программ. Задачи и цели обфускации. Оценка эффективности обфускации. Примеры обфускаторов программ, написанных на скриптовых языках. Способы и средства защиты программ от несанкционированного копирования. Защищенные операционные системы. Создание дистрибутива ОС Linux с повышенными требованиями к ее защищенности. Пример построения мобильной защищенной операционной системы на базе ОС Android.	18	
	Практическое занятие **Приложение 3.Практическое занятие №2, с. 202:** Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 202 — URL: https://urait.ru/bcode/543631/p.202 Решение разноуровневых заданий (задач): 1)Задания 1-16, с. 158 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. —	12	Устный (письменный) опрос, оценка навыка анализа и решения профессиональных задач

	(Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 158 — URL: https://urait.ru/bcode/543631/p.158 2)Задания 1-5, с. 156 Соколова, В. В. Разработка мобильных приложений : учебное пособие для среднего профессионального образования / В. В. Соколова. — Москва : Издательство Юрайт, 2021. — 160 с. — (Профессиональное образование). — ISBN 978-5-534-16868-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 156 — URL: https://urait.ru/bcode/542342/p.156		
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — С. 98 — 158 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543631/p.98-158 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-543631#page/158 - Средства, системы и комплексы защиты программного обеспечения 2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 126 — URL: https://urait.ru/bcode/542339/p.126 **Интерактивные формирующие тесты** 2. https://urait.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-542339#page/126 - Технологии разработки надежного программного обеспечения 3. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 21 с. — ISBN 978-5-906953-22- 3. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL:	5	Устный (письменный) опрос тестирование

	https://profspo.ru/books/98199. — Режим доступа: для авторизир. пользователей		
Тема 5. Исследование программного обеспечения на предмет отсутствия недекларированных возможностей	**Лекция** Сертификация средств защиты информации по требованиям безопасности информации. Проверка соответствия реальных и декларируемых функциональных возможностей. Проверка отсутствия недекларируемых возможностей. Контроль исходного состояния программного комплекса посредством утилиты «ФИКС». Статический анализ исходных текстов и исполняемых модулей ПО. Динамический анализ исходных текстов программ	20	
	Практическое занятие **Приложение 3. Лабораторная работа №1 – Фиксация программного комплекса, с. 204:** Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 204 — URL: https://urait.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-543631#page/204 **Приложение 3. Лабораторная работа №2 – Статический анализ исходных текстов на предмет полноты и отсутствия избыточности, с. 206:** Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 202 — URL: https://urait.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-543631#page/206 Решение разноуровневых заданий (задач): 1)Задания 1-12, с. 180 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 180 — URL: https://urait.ru/bcode/543631/p.180	20	Устный (письменный) опрос, оценка навыка анализа и решения профессиональных задач

	2) Задания 1-20, с. 227 Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 227 — URL: https://urait.ru/bcode/542339/p.227 3) Задания 1-8, с. 293 Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 293 — URL: https://urait.ru/bcode/542339/p.293		
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — С. 159 — 180 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543631/p.159-180 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-543631#page/180 - Исследование программного обеспечения на предмет отсутствия недекларированных возможностей	4	Устный (письменный) опрос тестирование
Тема 6. Краткое описание отечественных нормативных актов, регламентирующих деятельность в области защиты программного обеспечения	**Лекция** Федеральный закон «Об информации, информационных технологиях и о защите информации». ГОСТ Р ИСО/МЭК 15408—2013. ГОСТ Р ИСО/МЭК 18045—2013. ГОСТ Р МЭК 61508—2012. ГОСТ Р 56939—2016. Руководящий документ ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей». Приказ ФСТЭК России от 14 марта 2014 г. № 31. Требования к средствам антивирусной защиты ФСТЭК России. Банк данных угроз безопасности информации ФСТЭК России	24	

	Практическое занятие Решение разноуровневых заданий (задач): 1)Задания 1-6, с. 190 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 190 — URL: https://urait.ru/bcode/543631/p.190 2)Задания 1-6, с. 237 Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 237 — URL: https://urait.ru/bcode/542339/p.237	22	Устный (письменный) опрос, оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — С. 181 — 190 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543631/p.181-190 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-543631#page/190 - Краткое описание отечественных нормативных актов, регламентирующих деятельность в области защиты программного обеспечения	2	Устный (письменный) опрос тестирование
Тема 7. Вредоносные программы нового поколения	**Лекция** Особенности вредоносных программ нового поколения	6	
	Практическое занятие Решение разноуровневых заданий (задач): Задание 1, с. 32 Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2021. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 32 — URL:	6	Устный (письменный) опрос, оценка навыка анализа и решения профессиональных задач

	https://urait.ru/bcode/543873/p.32		
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — С. 196 — 313 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543631/p.196-313 2. *Советов, Б. Я.* Базы данных : учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 403 с. — (Профессиональное образование). — ISBN 978-5-534-18784-7. — С. 393 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/545704/p.393 **Интерактивные формирующие тесты** https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/32 - Угрозы Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2021. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 32 — URL: https://urait.ru/bcode/543873/p.32	2	Устный (письменный) опрос тестирование
	Консультация	5	
	Промежуточная аттестация – экзамен Итого:	270	

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Для проведения учебных занятий используются оборудованные техническими средствами кабинеты и лаборатории. Реализация учебной дисциплины МДК.02.01 Программные и программно-аппаратные средства обеспечения информационной безопасности осуществляется в лаборатории программных и программно-аппаратных средств защиты информации, в котором есть возможность проводить занятия, групповые и индивидуальные консультации, текущий контроль и промежуточную аттестацию, как в традиционной форме, так и с использованием интерактивных технологий и различных образовательных методик. Имеются также учебные аудитории для самостоятельной работы, кабинеты для проведения практических занятий, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования ФГОС СПО.

Оснащение лаборатории:

антивирусные программные комплексы;
программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
программные и программно-аппаратные средства обнаружения вторжений;
средства уничтожения остаточной информации в запоминающих устройствах;
программные средства выявления уязвимостей в АС и СВТ;
программные средства криптографической защиты информации;
программные средства защиты среды виртуализации.

Стол преподавательский, столы компьютерные, стулья; компьютер либо ноутбук с предустановленным стандартным программным обеспечением (по количеству обучающихся), широкополосный доступ в сеть Интернет, сетевой коммутатор, сетевая кабельная система. Используется либо свободно распространяемое программное обеспечение, либо поставляемое по лицензии образовательной организации; посадочные места по количеству обучающихся; рабочее место преподавателя; комплект учебно-наглядных пособий.

Технические средства обучения: для отображения презентаций используется проектор, стационарный или переносной экран либо интерактивная доска.

В колледже созданы все условия, позволяющие широко использовать в образовательном процессе информационные технологии, своевременно обеспечивать обновление нормативной документации, необходимой информации и оперативный доступ к ней. Установлены лицензионные программы, справочно-правовая система «КонсультантПлюс», программное обеспечение сетевого оборудования; обучающее программное обеспечение (среда программирования).

Учебники и учебные пособия по дисциплине МДК.02.01 Программные и программно-аппаратные средства обеспечения информационной безопасности находятся в свободном доступе для преподавателей и студентов в библиотеке колледжа. Библиотека колледжа оборудована рабочими местами в читальном зале и выходом в Интернет для работы с электронными книгами, учебниками, учебными пособиями.

При проведении синхронных и асинхронных занятий применяется электронная образовательная информационная среда учебного заведения на базе электронных образовательных платформ: «Profобразование», «Юрайт» и электронных образовательных ресурсов. Доступ к контенту и сервисам на образовательной платформам «Юрайт».

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543631
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542339

Дополнительная литература:

1. Внуков, *А. А.* Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования /А. А. Внуков. —3-еизд., перераб. И доп.— Москва: Издательство Юрайт, 2021.—161с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт].— URL: https://urait.ru/bcode/495525

2. Ворожейкин, В. Н. Технические средства и методы защиты информации – дополнительные главы : лабораторный практикум / В. Н. Ворожейкин. — 2-е изд. — Самара : Самарский государственный технический университет, ЭБС АСВ, 2019. — 336 с. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/111432 . — Режим доступа: для авторизир. пользователей
3. Долозов, Н. Л. Программные средства защиты информации : конспект лекций / Н. Л. Долозов, Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2015. — 63 с. — ISBN 978-5-7782-2753-8. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/91683. — Режим доступа: для авторизир. пользователей
4. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 21 с. — ISBN 978-5-906953-22-3. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/98199. — Режим доступа: для авторизир. пользователей
5. *Советов, Б. Я.* Базы данных : учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 403 с. — (Профессиональное образование). — ISBN 978-5-534-18784-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/545704
6. Соколова, В. В. Разработка мобильных приложений : учебное пособие для среднего профессионального образования / В. В. Соколова. — Москва : Издательство Юрайт, 2021. — 160 с. — (Профессиональное образование). — ISBN 978-5-534-16868-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542342
7. Щербак, А. В. Информационная безопасность :учебник для среднего профессионального образования / А. В. Щербак. —Москва :Издательство Юрайт,2021. —259 с. — (Профессиональное образование). —ISBN 978-5-534-15345-3.—Текст: электронный // Образовательная платформа Юрайт [сайт].—URL: https://urait.ru/bcode/497642
8. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).
9. ГОСТ 34.320-96.Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы иинформационной базы. 2001 г.www.standartgost.ru
10. ГОСТ Р ИСО/МЭК 15408—2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. – URL: https://docs.cntd.ru/document/1200105711
11. ГОСТ Р ИСО/МЭК 18045—2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 28 августа 2013 г. N 624-ст).
12. ГОСТ Р МЭК 61508—2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. – URL: https://docs.cntd.ru/document/1200102418
13. ГОСТ Р 56939—2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. – URL: https://docs.cntd.ru/document/1200135525
14. Руководящий документ ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей».
15. Приказ ФСТЭК России от 14 марта 2014 г. № 31. Требования к средствам антивирусной защиты ФСТЭК России. Банк данных угроз безопасности информации ФСТЭК России

Интернет-ресурсы:

1. Электронно-библиотечная система Юрайт [Электронный ресурс]. URL: https://urait.ru/

2. PROFобразование. Библиотека профессионала №1. URL: https://profspo.ru
3. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. URL: http://elibrary.ru
4. Национальная электронная библиотека [Электронный ресурс]. URL: https://нэб.рф/.
5. Электронно-библиотечная система «Университетская библиотека онлайн» [Электронный ресурс]. URL: http://biblioclub.ru
6. Официальный сайт компании «Консультант Плюс» URL: http://www.consultant.ru
7. Справочная правовая система «Гарант». URL: http://www.garant.ru 6.
8. Федеральный портал «Российское образование» [Электронный ресурс].URL: http://www.edu.ru

3.3 Образовательные технологии

Учебная деятельность обучающихся по дисциплине предусматривает учебные занятия (практическое занятие, лекция), самостоятельную работу, а также другие виды учебной деятельности.

В учебной деятельности по дисциплине используются различные образовательные технологии, в том числе:

синхронные занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана. На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс. Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

В смешанном обучении с применением дистанционных образовательных технологий студенты могут изучать лекционный материал в асинхронном режиме, готовить вопросы к занятиям семинарского типа.

Синхронные занятия семинарского (практического) типа

Занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса. Активность на занятиях оценивается по следующим критериям:

ответы на вопросы, предлагаемые преподавателем;

участие в дискуссиях;

выполнение разноуровневых заданий (задач).

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

В синхронном и асинхронном режиме используется сервис «Юрайт.Задания».

Асинхронные дистанционные занятия

В смешанном обучении с применением дистанционных образовательных технологий студенты могут осваивать лекционный материал в асинхронном режиме, готовить вопросы к синхронным семинарским (практическим) занятиям.

Для асинхронных занятий применяется следующая методика:

повторение и закрепление предыдущей темы (раздела);

изучение базовой и дополнительной рекомендуемой литературы, просмотр (прослушивание) медиаматериалов к новой теме (разделу);

тезисное конспектирование ключевых положений, терминологии, алгоритмов;

самостоятельная проверка освоения материала через интерактивный фонд оценочных средств (тесты);

выполнение рекомендуемых заданий;

фиксация возникающих вопросов и затруднений.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований и др.

Результаты обучения (освоенные умения, усвоенные знания)	**Коды формируемых профессиональных и общих компетенций**	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины обучающийся должен уметь: ~ формулировать требования к подсистеме защиты информации и к ее программно-аппаратным компонентам; ~ проектировать подсистему защиты информации в автоматизированной системе в части ее программно- аппаратных компонент защиты от несанкционированного доступа к информации, защиты от несанкционированного копирования информации, подсистем идентификации и аутентификации, защиты от разрушающих программных воздействий и защиты программного обеспечения от изучения; обосновывать необходимость применения тех или иных программно-аппаратных средств обеспечения информационной безопасности; обосновывать необходимость применения тех или иных программно-аппаратных средств обеспечения информационной безопасности; ~ работать с программно-аппаратными комплексами защиты информации: Secret Net 4.0, Dallas Lock 7.0 и Secret Disk Знать: ~ основы построения политики безопасности для различных систем; ~ как защитить ПЭВМ от локального несанкционированного доступа, как применять различные схемы идентификации и аутентификации, как защищать программы от несанкционированного копирования спомощью ключей; ~ как защитить КС от различных типов	ОК01, ОК02, ОК 03, ОК 04, ОК05, ОК 06, ОК 07, ОК08, ОК 09, ОК 10, ПК 2.1. ПК 2.4. ПК 2.5. ЛР1, ЛР 2, ЛР 4, ЛР 6, ЛР 7, ЛР 9, ЛР 13–18	Текущий контроль: - устный (письменный) опрос; Тестирование; оценка навыка анализа и решения профессиональных задач, самостоятельная работа.

разрушающих программных воздействий, в том числе файловых вирусов, загрузочных вирусов, программ типа «троянский конь»; как осуществлять регламентные работы, связанные с комплексным обеспечением информационной безопасности конкретных автоматизированных систем, и работ, осуществляемых в режимах нештатных ситуаций, в том числе мероприятий, - обязательных для автоматизированных систем, содержащих сведения, составляющие государственную тайну; - как обеспечить эффективное использование средств автоматического контроля, обнаружения и закрытия возможных каналов утечки конфиденциальных сведений		
Промежуточная аттестация		Экзамен
Форма контроля: может проводиться в форме тестирования, в письменной, а также в устной форме. Экзаменационные билеты по дисциплине могут включать теоретические вопросы, тестовые задания, разноуровневые задания (задачи).		

Рабочая программа учебной дисциплины

МДК.03.02 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Москва 2026

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н., _____
Протокол «102/168 от 28.08.2026»

СОДЕРЖАНИЕ

1. Паспорт программы учебной дисциплины
2. Структура и содержание дисциплины
3. Условия реализации дисциплины
4. Контроль и оценка результатов освоения дисциплины

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

1.1. Место дисциплины в структуре образовательной программы

Учебная дисциплина МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации, относится к профессиональному модулю ПМ.03 «Защита информации техническими средствами» профессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Дисциплина реализуется в традиционном формате, с использованием интерактивных форм проведения учебных занятий, в синхронном и асинхронном режиме на образовательной платформе ЮРАЙТ https://urait.ru/.

1.2. Цель и планируемые результаты освоения дисциплины

Содержание программы учебной дисциплины МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации направлено на достижение следующей цели - формирование знаний в области принципов добывания (разведки) информации, способов организационно-технической и технической защиты информации, активных и пассивных способов и средств скрытия и защиты, способов и средств технической дезинформации, принципов технического контроля защищенности объектов.

Результатом освоения программы является овладение обучающимися общими (ОК) и профессиональными (ПК) компетенциями, личностными результатами (ЛР):

Общие компетенции

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 08 . Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

Профессиональные компетенции

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей,

создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

Личностные результаты:

ЛР 1. Осознающий себя гражданином России и защитником Отечества, выражающий свою российскую идентичность в поликультурном и многоконфессиональном российском обществе и современном мировом сообществе. Сознающий свое единство с народом России, с Российским государством, демонстрирующий ответственность за развитие страны. Проявляющий готовность к защите Родины, способный аргументированно отстаивать суверенитет и достоинство народа России, сохранять и защищать историческую правду о Российском государстве.

ЛР 2. Проявляющий активную гражданскую позицию на основе уважения закона и правопорядка, прав и свобод сограждан, уважения к историческому и культурному наследию России. Осознанно и деятельно выражающий неприятие дискриминации в обществе по социальным, национальным, религиозным признакам; экстремизма, терроризма, коррупции, антигосударственной деятельности. Обладающий опытом гражданской социально значимой деятельности (в студенческом самоуправлении, добровольчестве, экологических, природоохранных, военно- патриотических и др. объединениях, акциях, программах). Принимающий роль избирателя и участника общественных отношений, связанных с взаимодействием с народными избранниками.

ЛР 4. Проявляющий и демонстрирующий уважение к труду человека, осознающий ценность собственного труда и труда других людей. Экономически активный, ориентированный на осознанный выбор сферы профессиональной деятельности с учетом личных жизненных планов, потребностей своей семьи, российского общества. Выражающий осознанную готовность к получению профессионального образования, к непрерывному образованию в течение жизни Демонстрирующий позитивное отношение к регулированию трудовых отношений. Ориентированный на самообразование и профессиональную переподготовку в условиях смены технологического уклада и сопутствующих социальных перемен. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 6. Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации.

ЛР 7. Осознающий и деятельно выражающий приоритетную ценность каждой человеческой жизни, уважающий достоинство личности каждого человека, собственную и чужую уникальность, свободу мировоззренческого выбора, самоопределения. Проявляющий бережливое и чуткое отношение к религиозной принадлежности каждого человека, предупредительный в отношении выражения прав и законных интересов других людей.

ЛР 9. Сознающий ценность жизни, здоровья и безопасности. Соблюдающий и пропагандирующий здоровый образ жизни (здоровое питание, соблюдение гигиены, режим занятий и отдыха, физическая активность), демонстрирующий стремление к физическому совершенствованию. Проявляющий сознательное и обоснованное неприятие вредных привычек и опасных наклонностей (курение, употребление алкоголя, наркотиков, психоактивных веществ, азартных игр, любых форм зависимостей), деструктивного поведения в обществе, в том числе в цифровой среде.

ЛР 13. Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности.

ЛР 14. Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.

ЛР 15.Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем.

ЛР 16. Соответствующий ожиданиям работодателей: креативно мыслящий, эффективно сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования,

распределяющий время и другие ресурсы для выполнения поставленной задачи в установленный срок, ответственный, дисциплинированный, целеустремленный, стрессоустойчивый.

ЛР 17. Демонстрирующий культуру речи, в том числе в деловой переписке/переговорах, способный презентовать себя и продукт профессиональной деятельности.

ЛР 18. Демонстрирующий способность использовать в цифровой среде различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.

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

Иметь практический опыт:

− установки, монтажа и настройки технических средств защиты информации;

− технического обслуживания технических средств защиты информации;

− применения основных типов технических средств защиты информации;

− выявления технических каналов утечки информации;

− участия в мониторинге эффективности технических средств защиты информации;

− диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;

− проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

− проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

− установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

Уметь:

− применять технические средства для криптографической защиты информации конфиденциального характера;

− применять технические средства для уничтожения информации и носителей информации;

− применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

− применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

− применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

− применять инженерно-технические средства физической защиты объектов информатизации

Знать:

− порядок технического обслуживания технических средств защиты информации;

− номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

− физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

− порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

− методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

− номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

− основные принципы действия и характеристики технических средств физической защиты;

− основные способы физической защиты объектов информатизации;

− номенклатуру применяемых средств физической защиты объектов информатизации.

2.СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Объем часов*
Максимальная учебная нагрузка (всего)	*270*
Обязательная аудиторная учебная нагрузка (всего)	*126*
в том числе:	
Лекции	*100*
практические занятия	*98*
Самостоятельная работа обучающегося (всего)	*48*
Промежуточная аттестация в форме итоговой работы	*7*

2.2. Тематический план и содержание дисциплины

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
Тема 1. Основные понятия и определения. Физические средства защиты информации	**Лекция** Физическая защита информации. Физическая защита данных.	10	
	Практические занятия Физическая защита информации. Физическая защита данных. Решение разноуровневых заданий (задач): 1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 16 — 32 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/23 2. Задания 1-14: Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт].с. 37 — URL: https://urait.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-542339#page/37	6	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы**	4	Устный (письменный)

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	по теме: 1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 16 — 32 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543873/p.16-32 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/23 - Введение в информационную безопасность		опрос
Тема 2. Модель угроз и модель нарушителя физической безопасности	**Лекция** Анализ возможных источников угроз безопасности. Модель нарушителя физической безопасности. Характеристика каналов утечки защищаемой информации. **Практические занятия** Модель угроз физической безопасности защищаемого объекта. Решение разноуровневых заданий (задач): *1., А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 237 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873?utm_campaign=rpd&utm_source=doc&utm_content=91cf0b6a61ed9e12b9fc43a33b74b999&#page/31 2. Задания 1-7: Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 47 — URL: https://urait.ru/bcode/542339/p.47	6 8	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва :	4	Устный (письменный) опрос

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 24 — 32 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543873/p.24-32 **Интерактивные формирующие тесты** https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/32 - Угрозы 2 Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 47 — URL: https://urait.ru/bcode/542339/p.47 **Интерактивные формирующие тесты** https://urait.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-542339?#page/47 - Угрозы надежности и безопасности программного обеспечения		
Тема 3. Проблемы безопасности интернет-протоколов	**Лекция** Введение в проблему безопасности интернет-протоколов. Протокол IP Протокол TCP Проблемы безопасности IP Маршрутизационные атаки Проблемы безопасности ICMP Проблемы безопасности ARP Проблемы безопасности IPv6 Проблемы безопасности UDP и TCP DNS NFS Электронная почта File Transfer Protocol Веб-приложения Динамические веб-сайты Куки Проблемы безопасности HTML5	12	
	Практические занятия Определение защищенной информационной системы Методология анализа защищенности информационной системы	4	Устный (письменный) опрос тестирование

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	Требования к архитектуре информационных систем для обеспечения безопасности ее функционирования Этапы построения системы безопасности ИС Решение разноуровневых заданий (задач): *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 56 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873?utm_campaign=rpd&utm_source=doc&utm_content=91cf0b6a61ed9e12b9fc43a33b74b999&#page/56		оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** **1.** *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 33 — 56 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873?utm_campaign=rpd&utm_source=doc&utm_content=91cf0b6a61ed9e12b9fc43a33b74b999&#page/33-56 **Интерактивные формирующие тесты** https://urait.ru/viewer/informacionnaya-bezopasnost-543873?utm_campaign=rpd&utm_source=doc&utm_content=91cf0b6a61ed9e12b9fc43a33b74b999&#page/56 - Проблемы безопасности интернет-протоколов	4	Устный (письменный) опрос
Тема 4. Построение системы безопасности	**Лекция** Общие принципы создания IT-систем. Структурный анализ. Определение потребности в защите. Анализ угроз. Анализ рисков. Архитектура безопасности. Базовые функции безопасности. Жизненный цикл безопасной разработки (Security Development Lifecycle).	10	
	Практические занятия Функции и задачи физической защиты. Проблемы защиты программного обеспечения информационных	6	Устный (письменный) опрос

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	систем. Жизненный цикл программного обеспечения ИС Решение разноуровневых заданий (задач): 1. Задание 1: Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт].с. 57-65 — URL: https://urait.ru/bcode/543873/p.65 **2.** Задания 1-7: Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт].с. 37 — URL: https://urait.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-542339#page/48		тестирование оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 33 — 65 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/65 **Интерактивные формирующие тесты** https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/65 - Построение системы безопасности	4	Устный (письменный) опрос
Тема 5. Описание объекта защиты. Определение категории важности информации.	**Лекция** Описание объекта защиты. Определение категории важности информации. Критерии оценки.	10	

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	Практические занятия Описание объекта защиты. Определение категории важности информации. Критерии оценки. Решение разноуровневых заданий (задач): *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 66 — 87 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/72	4	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 66 — 87 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543873/p.72 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/72 - Критерии оценки	4	Устный (письменный) опрос
Тема 6. Анализ нормативно-правовой базы физической защиты объекта информатизации.	**Лекция** Стандарты обеспечения информационной безопасности. Нормативно-правовая база физической защиты объекта информатизации.	10	
	Практические занятия Конституция РФ. Федеральные законы «О персональных данных» и «Об информации, информационных технологиях и о защите информации». Федеральный закон «Об электронной подписи». Решение разноуровневых заданий (задач): *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 248 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/248	8	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 238 — 248 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543873/p.238-248 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/248 - Правовые основы информационной безопасности	2	Устный (письменный) опрос
Тема 7. Модели безопасности	**Лекция** Матричная модель доступа. Модели, основанные на ролях. **Практические занятия** Модель «Китайская стена». Модель Белла-Лападулы Решение разноуровневых заданий (задач): *Задания 1-6: Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 87 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/87	10 4	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 73 — 87 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/73-87 **Интерактивные формирующие тесты** https://urait.ru/viewer/informacionnaya-bezopasnost-	2	Устный (письменный) опрос

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	543873?#page/87 - Модели безопасности		
Тема 8. Технологии работы с ключами	**Лекция** Введение в проблематику. Техники создания ключей. Иерархия ключей. **Практические занятия** Наивный протокол обмена ключами. Симметричные и ассиметричные алгоритмы обмена ключами. Решение разноуровневых заданий (задач): *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 100 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/100	10 4	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 88 — 100 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/88-100 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/100 - Технологии работы с ключами	2	Устный (письменный) опрос
Тема 9. Аутентификация. Биометрическая аутентификация	**Лекция** Введение в проблематику. Аутентификация на основе паролей. Использование одноразовых паролей для аутентификации. Методы «вызов-ответ». Аутентификация на основе обладания предметом. **Практические занятия** Аутентификация на основе паролей. Использование одноразовых паролей для аутентификации. Методы «вызов-ответ». Аутентификация на основе обладания предметом.	14 12	Устный (письменный) опрос тестирование оценка навыка

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	Решение разноуровневых заданий (задач): *1.Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 108 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/108 2. Задания 1-2: *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 108 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/120 3. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 125 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/125		анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** 1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 101 — 126 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/101-126 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/108 - Аутентификация на основе знания 2. https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/120 - Аутентификация на основе обладания предметом 3. https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/126- Биометрическая аутентификация	2	Устный (письменный) опрос
Тема 10. Особенности	**Лекция** Протокол RADIUS. AAA – архитектура.	10	

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
аутентификации в распределенных системах	Технология Blockchain. Биткойн – практическая реализация блокчейна. **Практические занятия** Протокол RADIUS. AAA – архитектура. Технология Blockchain. Биткойн – практическая реализация блокчейна. Решение разноуровневых заданий (задач): *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 134 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543873/p.134	8	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 127 — 134 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/127-134 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/134 - Особенности аутентификации в распределенных системах	2	Устный (письменный) опрос
Тема 11. Криптографическая защита информации.	**Лекция** Введение в проблематику. Шифры Цезаря, перестановки и перестановки «сцитала», Кардана. Магические квадраты. Симметричное и асимметричное шифрование. Безопасность методов шифрования. **Практические занятия** Шифры Цезаря, перестановки и перестановки «сцитала», Кардана. Магические квадраты. Симметричное и асимметричное шифрование. Безопасность методов шифрования. Решение разноуровневых заданий (задач): *Задания 1-14: Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. —	10 4	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональ

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 153 — 154 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/153-154		ных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 134 — 154 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/134-154 **Интерактивные формирующие тесты** https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/154- Основы криптографической защиты информации	2	Устный (письменный) опрос
Тема 12. Современные криптографические алгоритмы.	**Лекция** Введение в проблематику. Блочные шифры. Режимы шифрования. Поточные шифры. Понятие и свойства идеального шифра. Асимметричные шифры. RSA – алгоритм. Шифр Рабина. Обмен ключами Диффи-Хеллмана. Алгорим Эль-Гамаля. **Практические занятия** Блочные шифры. Режимы шифрования. Поточные шифры. Понятие и свойства идеального шифра. Асимметричные шифры. RSA –алгоритм. Шифр Рабина. Обмен ключами Диффи-Хеллмана. Алгорим Эль-Гамаля. Решение разноуровневых заданий (задач) 1-3: *1. Задания 1-3. Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 172 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/172 2. Задания 1-3: *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. —	10 4	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	(Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 178 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/178		
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** *1.Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 154 — 172 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/154-172 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/172 - Современные криптографические алгоритмы 2. https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/178- Электронная цифровая подпись	4	Устный (письменный) опрос
Тема 13. Безопасность сетей	**Лекция** Технология межсетевого экрана. Пакетные фильтры. Прокси межсетевые экраны. Фильтры приложений. Протоколы безопасной коммуникации. Виртуальная частная сеть. Электронная почта. GSM. GPRS. UMTS. WLAN. ZigBee. **Практические занятия** Технология межсетевого экрана. Пакетные фильтры. Прокси межсетевые экраны. Фильтры приложений. Протоколы безопасной коммуникации. Виртуальная частная сеть. Электронная почта. GSM. GPRS. UMTS. WLAN. ZigBee. Решение разноуровневых заданий (задач): *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 207 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/207	8 6	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** *1.Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования /	4	Устный (письменный) опрос

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 178 — 207 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/178-207 **2.** *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 208 — 227 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/208-227 **Интерактивные формирующие тесты** 1https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/207 - Безопасность сетей **2.** https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/227 - Безопасность мобильной и беспроводной связи		
Тема 14. Инженерно-техническая защита информации	**Лекция** Особая важность инженерно-технической защиты информации. Направления и методы инженерно-технической защиты информации. Средства технической охраны. Акустические, радиоэлектронные и оптические каналы утечки информации. **Практические занятия** Особая важность инженерно-технической защиты информации. Направления и методы инженерно-технической защиты информации. Средства технической охраны. Акустические, радиоэлектронные и оптические каналы утечки информации. Решение разноуровневых заданий (задач): *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 237 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-543873#page/237	6 5	Устный (письменный) опрос тестирование оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа обучающихся **Изучение основной и дополнительной литературы по теме:** *1.Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования /	2	Устный (письменный) опрос

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формы и методы контроля
	А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 227 — 237 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543873/p.227-237 **Интерактивные формирующие тесты** 1. https://urait.ru/viewer/informacionnaya-bezopasnost-543873?#page/237 - Инженерно-техническая защита информации		
	Итоговая работа	7	
	Итого	270	

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Для проведения учебных занятий используются оборудованные техническими средствами кабинеты и лаборатории. Реализация учебной дисциплины МДК.03.02
«Инженерно-технические средства физической защиты объектов информатизации» осуществляется в лаборатории «Технических средств защиты информации», в которой есть возможность проводить занятия, групповые и индивидуальные консультации, текущий контроль и промежуточную аттестацию, как в традиционной форме, так и с использованием интерактивных технологий и различных образовательных методик. Имеются также учебные аудитории для самостоятельной работы, кабинеты для проведения практических занятий, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования ФГОС СПО.

Оборудование лаборатории:

аппаратные средства аутентификации пользователя;

средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок;

средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.);

стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов.

компьютер либо ноутбук с предустановленным стандартным программным обеспечением (по количеству обучающихся), широкополосный доступ в сеть Интернет. Используется либо свободно распространяемое программное обеспечение, либо поставляемое по лицензии образовательной организации; посадочные места по количеству обучающихся; рабочее место преподавателя; комплект учебно-наглядных пособий.

Технические средства обучения: для отображения презентаций используется проектор, стационарный или переносной экран либо интерактивная доска.

В колледже созданы все условия, позволяющие широко использовать в образовательном процессе информационные технологии, своевременно обеспечивать обновление нормативной документации, необходимой информации и оперативный доступ к ней. Установлены лицензионные программы, справочно-правовая система
«КонсультантПлюс», программное обеспечение сетевого оборудования; обучающее программное обеспечение (среда программирования).

Учебники и учебные пособия по дисциплине МДК.03.02 «Инженерно-технические средства физической защиты объектов информатизации» находятся в свободном доступе для преподавателей и студентов в библиотеке колледжа. Библиотека колледжа оборудована рабочими местами в читальном зале и выходом в Интернет для работы с электронными книгами, учебниками, учебными пособиями.

При проведении синхронных и асинхронных занятий применяется электронная образовательная информационная среда учебного заведения на базе электронных образовательных платформ: «Юрайт» и электронных образовательных ресурсов.

3.2. Информационное обеспечение обучения

Для проведения учебных занятий используются оборудованные техническими средствами кабинеты и лаборатории. Реализация учебной дисциплины МДК.03.02 «Инженерно-технические средства физической защиты объектов информатизации» осуществляется в лаборатории «Технических средств защиты информации», в которой есть возможность проводить занятия, групповые и индивидуальные консультации, текущий контроль и промежуточную аттестацию, как в традиционной форме, так и с использованием интерактивных технологий и различных образовательных методик.

Имеются также учебные аудитории для самостоятельной работы, кабинеты для проведения практических занятий, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования ФГОС СПО.

Оборудование лаборатории: аппаратные средства аутентификации пользователя; средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок; средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.); стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов. Компьютер либо ноутбук с предустановленным стандартным программным обеспечением (по количеству обучающихся), широкополосный доступ в сеть Интернет.

Используется либо свободно распространяемое программное обеспечение, либо поставляемое по лицензии образовательной организации; посадочные места по количеству обучающихся; рабочее место преподавателя; комплект учебно-наглядных пособий.

Технические средства обучения: для отображения презентаций используется проектор, стационарный или переносной экран либо интерактивная доска.

В колледже созданы все условия, позволяющие широко использовать в образовательном процессе информационные технологии, своевременно обеспечивать обновление нормативной документации, необходимой информации и оперативный доступ ней. Установлены лицензионные программы, справочно-правовая система «КонсультантПлюс», программное обеспечение сетевого оборудования; обучающее программное обеспечение (среда программирования). Учебники и учебные пособия по дисциплине МДК.03.02 «Инженерно-технические средства физической защиты объектов информатизации» находятся в свободном доступе для преподавателей и студентов в библиотеке колледжа. Библиотека колледжа оборудована рабочими местами в читальном зале и выходом в Интернет для работы с электронными книгами, учебниками, учебными пособиями. При проведении синхронных и асинхронных занятий применяется электронная образовательная информационная среда учебного заведения на базе электронных образовательных платформ: «Юрайт» и электронных образовательных ресурсов.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — С. 227 — 237 — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543873/p.227-237
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт].с. 37

Дополнительная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/5423

Интернет-ресурсы

1. Образовательная платформа Юрайт. – URL: https://urait.ru
2. Национальная электронная библиотека https://нэб.рф/.
3. Федеральная служба по техническому и экспортному контролю: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty

3.3. Образовательные технологии

Учебная деятельность обучающихся по дисциплине предусматривает учебные занятия (практическое занятие, лекция), самостоятельную работу, а также другие виды учебной деятельности.

В учебной деятельности по дисциплине используются различные образовательные технологии, в том числе:

синхронные занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана. На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс. Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

В смешанном обучении с применением дистанционных образовательных технологий студенты могут изучать лекционный материал в асинхронном режиме, готовить вопросы к занятиям семинарского типа.

Синхронные занятия семинарского (практического) типа

Занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса. Активность на занятиях оценивается по следующим критериям:

ответы на вопросы, предлагаемые преподавателем;

участие в дискуссиях;

выполнение разноуровневых заданий (задач).

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

В синхронном и асинхронном режиме используется сервис «Юрайт.Задания».

Асинхронные дистанционные занятия

В смешанном обучении с применением дистанционных образовательных технологий студенты могут осваивать лекционный материал в асинхронном режиме, готовить вопросы к синхронным семинарским (практическим) занятиям.

Для асинхронных занятий применяется следующая методика:

повторение и закрепление предыдущей темы (раздела);

изучение базовой и дополнительной рекомендуемой литературы, просмотр (прослушивание) медиаматериалов к новой теме (разделу);

тезисное конспектирование ключевых положений, терминологии, алгоритмов;

самостоятельная проверка освоения материала через интерактивный фонд оценочных средств (тесты);

выполнение рекомендуемых заданий;

фиксация возникающих вопросов и затруднений.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения семинарских и практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований и др.

Результаты обучения (освоенные умения, усвоенные знания)	**Коды формируемых профессиональных и общих компетенций**	**Формы и методы контроля и оценки результатов обучения**
Иметь практический опыт: − установки, монтажа и настройки технических средств защиты информации;	ОК01, ОК02, ОК 03, ОК 04,	Текущий контроль: - устный (письменный) опрос; Тестирование;

− технического обслуживания технических средств защиты информации; − применения основных типов технических средств защиты информации; − выявления технических каналов утечки информации; − участия в мониторинге эффективности технических средств защиты информации; − диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; − проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; − проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; − установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. Уметь: − применять технические средства для криптографической защиты информации конфиденциального характера; − применять технические средства для уничтожения информации и носителей информации; − применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;	ОК05, ОК 06, ОК 07, ОК08, ОК 09, ПК 3.1-3.5 ЛР1, ЛР 2, ЛР 4, ЛР 6, ЛР 7, ЛР 9, ЛР 13–18	оценка навыка анализа и решения профессиональных задач, самостоятельная работа.

− применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; − применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; − применять инженерно-технические средства физической защиты объектов информатизации Знать: − порядок технического обслуживания технических средств защиты информации; − номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; − физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; − порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; − методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; − номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; − основные принципы действия и характеристики технических средств физической защиты; − основные способы физической защиты объектов		

информатизации; − номенклатуру применяемых средств физической защиты объектов информатизации.		

РАБОЧАЯ ПРОГРАММА

учебной дисциплины
ОПЦ.03 ОСНОВЫ АЛГОРИТМИЗАЦИИ И ПРОГРАММИРОВАНИЯ

для специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем
(базовая подготовка)
на базе основного общего образования

Рабочая программа разработана на основе требований Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем", утвержденного приказом Минобрнауки России от 09.12.2016 N 1553 (ред. от 17.12.2020)

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н., _____

Протокол «102/168 от 28.08.2026»

СОДЕРЖАНИЕ

1.	**ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**	**4**
2.	**СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**	**4**
3.	**УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**	**7**
4.	**КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**	**8**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОПЦ.03 ОСНОВЫ АЛГОРИТМИЗАЦИИ И ПРОГРАММИРОВАНИЯ

1.1. Место дисциплины в структуре основной профессиональной образовательной программы: Общепрофессиональный цикл.

1.2. Цель и планируемые результаты освоения дисциплины:

Код ПК, ОК	Умения	Знания
ОК 01; ОК 02; ОК 09; ПК 2.2.; ПК 2.3.; ПК 2.4.;	Разрабатывать алгоритмы для конкретных задач. Использовать программы для графического отображения алгоритмов. Определять сложность работы алгоритмов. Работать в среде программирования. Реализовывать построенные алгоритмы в виде программ на конкретном языке программирования. Оформлять код программы в соответствии со стандартом кодирования. Выполнять проверку, отладку кода программы.	Понятие алгоритмизации, свойства алгоритмов, общие принципы построения алгоритмов, основные алгоритмические конструкции. Эволюцию языков программирования, их классификацию, понятие системы программирования. Основные элементы языка, структуру программы, операторы и операции, управляющие структуры, структуры данных, файлы, классы памяти. Подпрограммы, составление библиотек подпрограмм. Объектно-ориентированную модель программирования, основные принципы объектно-ориентированного программирования на примере алгоритмического языка: понятие классов и объектов, их свойств и методов, инкапсуляции и полиморфизма, наследования и переопределения.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОПЦ.03 ОСНОВЫ АЛГОРИТМИЗАЦИИ И ПРОГРАММИРОВАНИЯ»

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объём в часах**
Объем образовательной программы	252
в том числе:	180
теоретическое обучение	94
практические занятия	76
Самостоятельная работа	40,8
Промежуточная аттестация - экзамен	**4**

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	*Содержание учебного материала и формы организации деятельности обучающихся*	*Объём в часах*	*Коды компетенций, формированию которых способствует элемент программы*
1	**2**	**3**	**4**
Тема 1. Основы алгоритмизации, языки и системы программирования.	***Содержание учебного материала***	**30**	ОК 01; ОК 02; ОК 09; ПК 2.2.; ПК 2.3.; ПК 2.4.;
	Вводная лекция.		
	Основы алгоритмизации.		
	Алгоритмы цикла.		
	Основы алгоритмизации.		
	Языки и системы программирования		
	Алгоритмы. Языки программирования		
	Тематика практических занятий и лабораторных работ		
	Самостоятельная работа обучающихся		
Тема 2. Основные элементы языка. Управляющие операторы языка. Структурированные типы данных. Символьные типы данных	***Содержание учебного материала***	**32**	ОК 01; ОК 02; ОК 09; ПК 2.2.; ПК 2.3.; ПК 2.4.;
	Основные элементы языка. Операторы языка. Ввод/вывод данных.		
	Управляющие операторы языка. Операторы выбора. Оператор условной передачи управления. Оператор безусловной передачи управления.		
	Оператор case. Операторы организации циклической обработки. Циклы.		
	Структуры данных. Массивы. Работа с массивами. Одномерные массивы. Обработка массивов. Сортировка массивов. Двумерные массивы. Решение систем уравнений.		
	Коллекции. Контейнеры. Операции над коллекциями и контейнерами. Обработка коллекций. Многомерные контейнеры. Обработка контейнеров.		
	Символьные типы данных. Символы и строки. Обработка символов. Обработка строк.		
	Строковые массивы. Файлы. Потоки. Считывание из файла. Запись в файл. Редактирование файлов.		
	Тематика практических занятий и лабораторных работ		
	Самостоятельная работа обучающихся		
Тема 3. Модульное программирование. Рекурсия. Визуально-событийно	Содержание учебного материала	**32**	ОК 01; ОК 02; ОК 09; ПК 2.2.;
	Локальные и глобальные переменные. Модульное программирование.		
	Процедуры и функции. Подпрограммы. Передача данных в процедуры и функции.		

управляемое программирование. Разработка оконного приложения	Рекурсия. Разработка рекурсивных подпрограмм		ПК 2.3.; ПК 2.4.;
	Визуально-событийно управляемое программирование.		
	Виджеты. События. Основные элементы управления.		
	Разработка оконного приложения.		
	Установка приложения		
	Тематика практических занятий и лабораторных работ		
	Самостоятельная работа обучающихся		
В том числе, практических работ: 1. Операторы выбора 2. Циклы 3. Работа с массивами 4. Коллекции и контейнеры 5. Символы и строки 6. Работа с файлами 7. Реализация подпрограммы. 8. Разработка рекурсивных подпрограмм. 9. Основные элементы управления. 10. Разработка оконного приложения.		**76**	
Самостоятельная работа обучающихся: подготовка к практическим работам		**40,8**	
Промежуточная аттестация, в т.ч. **Консультация** **Экзамен**		 ***2*** ***4***	
Всего:		***252***	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОПЦ.03 ОСНОВЫ АЛГОРИТМИЗАЦИИ И ПРОГРАММИРОВАНИЯ

3.1. Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Лаборатория «Программного обеспечения компьютерных сетей, программирования и баз данных», оснащенная необходимым для реализации программы учебной дисциплины оборудованием:

- 12-15 компьютеров обучающихся и 1 компьютер преподавателя (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i3, оперативная память объемом не менее 8 Гб; HD 500 Gb или больше программное обеспечение: операционные системы Windows, UNIX, пакет офисных программ, пакет САПР);
- Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа, обжимной инструмент, коннекторы RJ-45, тестеры для кабеля, кросс-ножи, кросс-панели;
- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности
- Сервер в лаборатории (аппаратное обеспечение: не менее 2 сетевых плат, 8-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 2 Тб, программное обеспечение:WindowsServer 2012 или более новая версия, лицензионные антивирусные программы, лицензионные программы восстановления данных, лицензионный программы по виртуализации.)
- Технические средства обучения:
- Компьютеры с лицензионным программным обеспечением
- Интерактивная доска
- Проектор

3.2. Информационное обеспечение реализации программы

Основная литература

1. Трофимов, В. В. Основы алгоритмизации и программирования : учебник для среднего профессионального образования / В. В. Трофимов, Т. А. Павловская ; под редакцией В. В. Трофимова. — Москва : Издательство Юрайт, 2022. — 137 с. — (Профессиональное образование). — ISBN 978-5-534-07321-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493261

2. Кудрина, Е. В. Основы алгоритмизации и программирования на языке C# : учебное пособие для среднего профессионального образования / Е. В. Кудрина, М. В. Огнева. — Москва : Издательство Юрайт, 2022. — 322 с. — (Профессиональное образование). — ISBN 978-5-534-10772-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494914

3. Паронджанов, В. Д. Алгоритмические языки и программирование: ДРАКОН : учебное пособие для среднего профессионального образования / В. Д. Паронджанов. — Москва : Издательство Юрайт, 2022. — 436 с. — (Профессиональное образование). — ISBN 978-5-534-14733-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497329

Дополнительная литература

1. Огнева, М. В. Программирование на языке C++: практический курс : учебное пособие для среднего профессионального образования / М. В. Огнева, Е. В. Кудрина. — Москва : Издательство Юрайт, 2022. — 335 с. — (Профессиональное образование). —

ISBN 978-5-534-05780-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493047

2. Черпаков, И. В. Основы программирования : учебник и практикум для среднего профессионального образования / И. В. Черпаков. — Москва : Издательство Юрайт, 2022. — 219 с. — (Профессиональное образование). — ISBN 978-5-9916-9984-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491068

3. Федоров, Д. Ю. Программирование на языке высокого уровня Python : учебное пособие для среднего профессионального образования / Д. Ю. Федоров. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 210 с. — (Профессиональное образование). — ISBN 978-5-534-12829-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/492921

Интернет-ресурсы

1.Изучаем алгоритмы: полезные книги, веб-сайты, онлайн-курсы и видеоматериалы - https://proglib.io/p/awesome-algorithms

2. Школа программиста - https://acmp.ru/

3. Задачки, упражнения и соревнования для начинающих и опытных кодеров - https://gb.ru/posts/resources_for_programming_practice

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ ОПЦ.03 ОСНОВЫ АЛГОРИТМИЗАЦИИ И ПРОГРАММИРОВАНИЯ

Результаты обучения	***Критерии оценки***	***Формы и методы оценки***
Перечень знаний, осваиваемых в рамках дисциплины:	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены,	Оценка в рамках текущего контроля результатов выполнения индивидуальных контрольных заданий, результатов выполнения практических работ, устный индивидуальный опрос. Письменный опрос в форме тестирования

Понятие алгоритмизации, свойства алгоритмов, общие принципы построения алгоритмов, основные алгоритмические конструкции. Эволюцию языков программирования, их классификацию, понятие системы программирования. Основные элементы языка, структуру программы, операторы и операции, управляющие структуры, структуры данных, файлы, классы памяти. Подпрограммы, составление библиотек подпрограмм. Объектно-ориентированную модель программирования, основные принципы объектно-ориентированного программирования на примере алгоритмического языка: понятие классов и объектов, их свойств и методов, инкапсуляции и полиморфизма, наследования и переопределения.	некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	
Перечень умений, осваиваемых в рамках дисциплины:		
Разрабатывать алгоритмы для конкретных задач. Использовать программы для графического отображения алгоритмов. Определять сложность работы алгоритмов. Работать в среде программирования. Реализовывать построенные алгоритмы в виде программ на конкретном языке программирования. Оформлять код программы в соответствии со стандартом кодирования. Выполнять проверку, отладку кода программы.		Экспертное наблюдение и оценивание выполнения практических работ. Текущий контроль в форме защиты практических работ

РАБОЧАЯ ПРОГРАММА

учебной дисциплины
ОПЦ.07 Технические средства информатизации
для специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем
(базовая подготовка)
на базе основного общего образования

Рабочая программа разработана на основе требований Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Зарегистрировано в Минюсте России 09.12.2016 N 1553) (ред. от 17.12.2020)

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н.,
Протокол «102/168 от 28.08.2026»

СОДЕРЖАНИЕ

1	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2	РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
3	СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	8
4	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	21
5	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)	23

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля (далее – рабочая программа) является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности (специальностям) СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида профессиональной деятельности (ВПД) ПМ.03. Защита информации техническими средствами и соответствующих **профессиональных компетенций (ПК):**

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

ПРОИЗВОДСТВЕННАЯ (ПРЕДДИПЛОМНАЯ) ПРАКТИКА

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-
аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах
отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-
аппаратных средств защиты информации.

ПК 2.4.Осуществлять обработку, хранение и передачу информации ограниченного
доступа.

ПК 2.5.Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6.Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

ПК 4.1.Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного
обеспечения

ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами,
таблицами, презентациями и содержанием баз данных, работать в графических редакторах

ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и
сервисов Интернета

ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной
Системе.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

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

иметь практический опыт:

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;
- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;
- проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
- проведения измерений параметров фоновых шумов, а также физических

полей, создаваемых техническими средствами защиты информации;

− установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

уметь:

− применять технические средства для криптографической защиты информации конфиденциального характера;
− применять технические средства для уничтожения информации и носителей информации;
− применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническимисредствами;
− применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
− применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
− применять инженерно-технические средства физической защиты объектов информатизации

знать:

− порядок технического обслуживания технических средств защиты информации;
− номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
− физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей итехнических каналов утечки информации;
− порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;
− методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
− номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
− основные принципы действия и характеристики технических средств физической защиты;
− основные способы физической защиты объектов информатизации;
− номенклатуру применяемых средств физической защиты объектов информатизации.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля

Всего – 720 часов, в том числе:

- максимальная учебная нагрузка обучающегося – 720 часа, включая:
- обязательную аудиторную учебную нагрузку обучающегося – 588 часа;
- самостоятельную работу обучающегося – 102 часа;
- учебная и производственная практика – 216 часов;
- промежуточная аттестация – 18 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности: обеспечение проектной деятельности, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование видов деятельности и профессиональных компетенций
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды общих и профессиональных компетенций	**Наименования разделов профессионального модуля****	**Всего часов** (макс.учебная нагрузка и практика)	**Объем часов, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося:**		**Учебная, часов**	**Производственная (по профилю специальности),** часов (если предусмотрена рассредоточенная практика)
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч. курсовая работа (проект),**часов	**Всего,** часов	**в т.ч. курсовая работа (проект),**часов		
1	2	3	4	5	6	7	8	9	10
ПК 3.1 – ПК 3.5	Раздел 1. МДК.03.01 Техническая защита информации	**216**	**162**	78	-	**54**			**-**
	Раздел 2. МДК.03.02 Инженерно-технические средства физической защиты объектов информации	**270**	**206**	98	18	**48**			**-**
	Учебная практика	**72**						**72**	
	Производственная практика (по профилю специальности), часов	**144**							**144**
	Промежуточная аттестация МДК.03.01 [1]	**18**							**-**
	Всего:	**720**	**588**	176	18	**102**		**72**	**144**

[1] Выбор формы промежуточной аттестации в основных образовательных программах определяется образовательной организацией самостоятельно.

3.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
МДК.03.01 Техническая защита информации		**216**
Раздел 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание учебного материала:** 1. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные параметры системы защиты информации.	2
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание учебного материала:** 1. Задачи и требования к способам и средствам защиты информации техническими средствами. 2. Принципы системного анализа проблем инженерно-технической защиты информации. 3. Классификация способов и средств защиты информации.	6
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	**Содержание учебного материала:** 1. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. 2. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. 3. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	6
	Практические занятия Практическая работа № 1. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. Практическая работа № 2. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. Практическая работа № 3. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	8

	Самостоятельная работа обучающегося: Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	4
Тема 2.2. Технические каналы утечки информации	**Содержание учебного материала:** 1. Понятие и особенности утечки информации. Структура канала утечки информации. 2. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. 3.Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	6
	Практические занятия Практическая работа № 4. Угрозы информационной безопасности. Практическая работа № 5. Угрозы информационной безопасности. Практическая работа № 6. Угрозы информационной безопасности.	8
Тема 2.3. Методы и средства технической разведки	**Содержание учебного материала:** 1. Классификация технических средств разведки. Методы и средства технической разведки. 2.Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. 3.Средства дистанционного съема информации.	6
	Практические занятия Практическая работа № 7. Организация аттестации выделенного помещения по требованиям безопасности информации. Практическая работа № 8. Организация аттестации выделенного помещения по требованиям безопасности информации.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Раздел 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание учебного материала:** 1. Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. 2. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. 3. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. 4. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей.	6
	Практические занятия Практическая работа № 9. Измерение параметров физических полей. Практическая работа № 10. Измерение параметров физических полей.	8

	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание учебного материала:** 1. Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. 2. Экранирование. Зашумление.	6
	Практические занятия Практическая работа № 11. Защита аппаратуры от электромагнитных полей. Практическая работа № 12. Защита аппаратуры от электромагнитных полей. Практическая работа № 13. Защита аппаратуры от электромагнитных полей.	8
	Самостоятельная работа обучающегося: Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	4
Раздел 4. Системы защиты от утечки информации		
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание учебного материала:** 1. Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. 2. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу. ОКР	6
	Практические занятия Практическая работа № 14. Защита от утечки по акустическому каналу. Практическая работа № 15. Защита от утечки по акустическому каналу.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание учебного материала:** 1. Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. 2. Негласная запись информации на диктофоны. Системы защиты от диктофонов. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	6
	Практические занятия Практическая работа № 16. Системы защиты от утечки информации по проводному каналу. Практическая работа № 17. Системы защиты от утечки информации по проводному каналу.	8

Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание учебного материала:** 1. Электронные стетоскопы. Лазерные системы подслушивания. 2. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	6
	Практические занятия Практическая работа № 18. Защита от утечки по виброакустическому каналу. Практическая работа № 19. Защита от утечки по виброакустическому каналу.	8
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание учебного материала:** 1. Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. 2. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладках. 3. Системы защиты от утечки по электромагнитному каналу. 4. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	6
	Практические занятия Практическая работа № 20. Определение каналов утечки ПЭМИН. Практическая работа № 21. Определение каналов утечки ПЭМИН. Практическая работа № 22. Защита от утечки по цепям электропитания и заземления. Практическая работа № 23. Защита от утечки по цепям электропитания и заземления.	8
	Самостоятельная работа обучающегося: Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	4
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание учебного материала:** 1. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. 2. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	6
	Практические занятия Практическая работа № 24. Технические средства защиты информации в телефонных линиях. Практическая работа № 25. Технические средства защиты информации в телефонных линиях.	8

	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание учебного материала:** 1. Низкочастотное устройство съема информации. 2. Высокочастотное устройство съема информации. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	6
	Практические занятия Практическая работа № 26. Системы защиты от утечки информации по электросетевому каналу. Практическая работа № 27. Системы защиты от утечки информации по электросетевому каналу.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание учебного материала:** 1. Телевизионные системы наблюдения. Приборы ночного видения. 2. Системы защиты информации по оптическому каналу.	8
	Практические занятия Практическая работа № 28. Системы защиты от утечки информации по оптическому каналу	8
	Самостоятельная работа обучающегося: Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	4
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение технических средств защиты информации	**Содержание учебного материала:** 1. Технические средства для уничтожения информации и носителей информации, порядок применения. 2. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. 3. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. 4. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. 5. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	8
	Практические занятия Практическая работа № 29. Применение технических средств защиты информации. Практическая работа № 30. Применение технических средств защиты информации. Практическая работа № 31. Применение технических средств защиты информации.	8

	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание учебного материала:** 1. Этапы эксплуатации технических средств защиты информации. 2. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. 3. Установка и настройка технических средств защиты информации. 4. Установка и настройка технических средств защиты информации. 5. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. 6. Организация ремонта технических средств защиты информации. 7. Проведение аттестации объектов информатизации.	8
	Практические занятия Практическая работа № 32. Эксплуатация технических средств защиты информации. Практическая работа № 33. Эксплуатация технических средств защиты информации.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Промежуточная аттестация по МДК.03.01 в форме экзамена		**18**
Учебная практика по МДК.03.01 **Виды работ:** ~ Измерение параметров физических полей. ~ Определение каналов утечки ПЭМИН. ~ Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. ~ Установка и настройка технических средств защиты информации. ~ Проведение измерений параметров побочных электромагнитных излучений и наводок. ~ Проведение аттестации объектов информатизации.		
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**270**
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание учебного материала:** 1. Характеристики потенциально опасных объектов. 2. Содержание и задачи физической защиты объектов информатизации. 3. Содержание и задачи физической защиты объектов информатизации. 4. Основные понятия инженерно-технических средств физической защиты. 5. Основные понятия инженерно-технических средств физической защиты. 6. Категорирование объектов информатизации. 7. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.	10

	8. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. 9. Особенности задач охраны различных типов объектов. 10. Особенности задач охраны различных типов объектов.	
	Тематика практических занятий и лабораторных работ Практическая работа № 1. Характеристика объекта защиты. Практическая работа № 2. Характеристика объекта защиты. Практическая работа № 3. Характеристика объекта защиты.	8
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание учебного материала:** 1. Общие принципы обеспечения безопасности объектов. 2. Жизненный цикл системы физической защиты. 3. Жизненный цикл системы физической защиты. 4. Принципы построения интегрированных систем охраны. 5. Принципы построения интегрированных систем охраны. 6. Классификация и состав интегрированных систем охраны. 7. Классификация и состав интегрированных систем охраны. 8. Требования к инженерным средствам физической защиты. 9. Требования к инженерным средствам физической защиты. 10. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. 11. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	10
	Практические занятия Практическая работа № 4. Анализ нормативно-правовой базы физической защиты. Практическая работа № 5. Анализ нормативно-правовой базы физической защиты. Практическая работа № 6. Анализ нормативно-правовой базы физической защиты. Практическая работа № 7. Формирование требований к физической защите объекта. Практическая работа № 8. Формирование требований к физической защите объекта. Практическая работа № 9. Формирование требований к физической защите объекта	10
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	6
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание учебного материала:** 1. Информационные основы построения системы охранной сигнализации. 2. Информационные основы построения системы охранной сигнализации. 3. Назначение, классификация технических средств обнаружения. 4. Назначение, классификация технических средств обнаружения.	10

	5. Построение систем обеспечения безопасности объекта. 6. Построение систем обеспечения безопасности объекта. 7. Построение систем обеспечения безопасности объекта. 8. Периметровые средства обнаружения: назначение, устройство, принцип действия. 9. Периметровые средства обнаружения: назначение, устройство, принцип действия. 10. Периметровые средства обнаружения: назначение, устройство, принцип действия. 11. Объектовые средства обнаружения: назначение, устройство, принцип действия. 12. Объектовые средства обнаружения: назначение, устройство, принцип действия. ОКР.	
	Практические занятия Практическая работа № 10. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 11. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 12. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 13. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 14. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 15. Монтаж датчиков пожарной и охранной сигнализации.	10
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	6
Тема 2.2. Система контроля и управления доступом	**Содержание учебного материала:** 1. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. 2. Особенности построения и размещения СКУД. 3. Структура и состав СКУД. 4. Периферийное оборудование и носители информации в СКУД. 5. Основы построения и принципы функционирования СКУД. 6. Классификация средств управления доступом. 7. Средства идентификации и аутентификации. 8. Методы удостоверения личности, применяемые в СКУД. 9. Методы удостоверения личности, применяемые в СКУД. 10. Обнаружение металлических предметов и радиоактивных веществ.	10
	Практические занятия Практическая работа № 16. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя. Практическая работа № 17. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя Практическая работа № 18. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя.	10

	Практическая работа № 19. Рассмотрение принципов устройства, работы и применения средств контроля доступа. Практическая работа № 20. Рассмотрение принципов устройства, работы и применения средств контроля доступа.	
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Тема 2.3. Система телевизионного наблюдения	**Содержание учебного материала:** 1. Аналоговые и цифровые системы видеонаблюдения. 2. Назначение системы телевизионного наблюдения. 3. Состав системы телевизионного наблюдения. 4. Видеокамеры. 5. Объективы. 6. Термокожухи. 7. Поворотные системы. 8. Инфракрасные осветители. 9. Детекторы движения.	8
	Практические занятия Практическая работа № 21. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. Практическая работа № 22. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. Практическая работа № 23. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. Практическая работа № 24. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	10
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание учебного материала:** 1. Классификация системы сбора и обработки информации. 2. Классификация системы сбора и обработки информации. 3. Схема функционирования системы сбора и обработки информации. 4. Схема функционирования системы сбора и обработки информации.	8

	5. Варианты структур построения системы сбора и обработки информации. 6. Варианты структур построения системы сбора и обработки информации. 7. Устройства отображения и документирования информации.	
	Практические занятия Практическая работа № 25. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. Практическая работа № 26. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. Практическая работа № 27. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. Практическая работа № 28. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	10
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Тема 2.5 Система воздействия	**Содержание учебного материала:** 1. Назначение и классификация технических средств воздействия. 2. Назначение и классификация технических средств воздействия. 3. Основные показатели технических средств воздействия. 4. Основные показатели технических средств воздействия.	10
	Практические занятия Практическая работа № 29. Выбор и обоснование средств подсистемы задержки. Практическая работа № 30. Выбор и обоснование средств подсистемы задержки. Практическая работа № 31. Выбор и обоснование средств подсистемы задержки.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		**73**

Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание учебного материала:** 1. Периметровые и объектовые средства обнаружения, порядок применения. 2. Работа с периферийным оборудованием системы контроля и управления доступом. 3. Особенности организации пропускного режима на КПП. 4. Управление системой телевизионного наблюдения с автоматизированного рабочего места. 5. Порядок применения устройств отображения и документирования информации. 6. Управление системой воздействия. ОКР.	10
	Практические занятия Практическая работа № 32. Разработка структурной схемы и спецификации оборудования Практическая работа № 33. Разработка структурной схемы и спецификации оборудования Практическая работа № 34. Разработка структурной схемы и спецификации оборудования Практическая работа № 35. Разработка структурной схемы и спецификации оборудования	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	6
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание учебного материала:** 1. Этапы эксплуатации. 2. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. 3. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. 4. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. 5. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. 6. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. 7. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. 8. Организация ремонта технических средств физической защиты. Дифференцированный зачет.	10
	Практические занятия Практическая работа № 36. Эксплуатация инженерно-технических средств физической защиты. Практическая работа № 37. Эксплуатация инженерно-технических средств физической защиты Практическая работа № 38. Эксплуатация инженерно-технических средств физической защиты Практическая работа № 39. Эксплуатация инженерно-технических средств физической защиты Практическая работа № 40. Эксплуатация инженерно-технических средств физической защиты	10

	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Обязательная аудиторная учебная нагрузка по курсовой работе		**18**
Примерная тематика курсовых работ: 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества. 4. Основные операции проведения технического обслуживания инженерно-технических средств физической защиты. 5. Размещение периметровых средств обнаружения на местности.		
Учебная практика по разделу по МДК.03.02 1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации.		***72***
Производственная практика профессионального модуля ПМ.03 **Виды работ** 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.		***144***
Экзамен по профессиональному модулю		***18***
Всего		***720***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к материально-техническому обеспечению

Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Компьютерные классы: парты, столы, стулья, компьютерные столы, интерактивная доска, компьютеры, в составе локальной вычислительной сети факультета, подключенной к интернет, сетевое оборудование.

Adobe Reader, Microsoft Office, SP3,Браузеры (Chrome, FireFox)

Лаборатория «Технических, программных и программно-аппаратных средств защиты информации»

Лабораторный стенд «Защита информации от утечек по акустовибрационным каналам», Типовой комплект учебного оборудования «Сетевая безопасность» SECURITY.

3.2. Информационное обеспечение реализации программы

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

3.2.1 Электронные издания (электронные ресурсы)

Основные источники

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518006.

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519364

3. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519614

Дополнительные источники

1. Толстобров, А. П. Архитектура ЭВМ : учебное пособие для среднего профессионального образования / А. П. Толстобров. — 2-е изд., испр. идоп. — М.: Издательство Юрайт, 2021. — 154 с. — (Профессиональное

образование). — ISBN 978-5-534-13398-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/476555

2. Новожилов, О. П. Архитектура компьютерных систем в 2 ч. Часть1 : учебное пособие для среднего профессионального образования / О. П. Новожилов. — М.: Издательство Юрайт, 2021. — 276 с. — (Профессиональное образование). — ISBN 978-5-534-10299-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/475573

3. Новожилов, О. П. Архитектура компьютерных систем в 2 ч. Часть2 : учебное пособие для среднего профессионального образования / О. П. Новожилов. — М.: Издательство Юрайт, 2021. — 246 с. — (Профессиональное образование). — ISBN 978-5-534-10301-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/475574

3.2.2. Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей; https://ichip.ru/
2. Журналы Защита информации. Инсайд: Информационно-методический журнал. http://www.inside-zi.ru/
3. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. http://cyberrus.com/
4. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. http://bit.mephi.ru/

3.2.3. Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Российский биометрический портал www.biometrics.ru
4. Сайт журнала Информационная безопасность http://www.itsec.ru
5. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
6. Федеральный портал «Информационно-коммуникационные технологии в образовании» http://window.edu.ru/
7. Федеральный портал «Российское образование» www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов

		выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

РАБОЧАЯ ПРОГРАММА

учебной дисциплины
ПМ.01. ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ
для специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем
(базовая подготовка)
на базе основного общего образования

Рабочая программа разработана на основе требований Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Зарегистрировано в Минюсте России 09.12.2016 N 1553) (ред. от 17.12.2020)

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н.,
Протокол «102/168 от 28.08.2026»

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА:

1	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02	4
2	РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
3	СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА: ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	8
4	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	30
5	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)	32

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля (далее – рабочая программа) является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности (специальностям) СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида профессиональной деятельности (ВПД) ПМ.01. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующих **профессиональных компетенций (ПК):**

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении

1.2. Цели и задачи модуля – требования к результатам освоения модуля

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

иметь практический опыт:

- эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;
- администрировании автоматизированных систем в защищенном исполнении;
- установке компонентов систем защиты информации автоматизированных информационных систем.

уметь:

- обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;
- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации

автоматизированной системы;
- организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;
- настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

знать:

- состав и принципы работы автоматизированных систем, операционных систем и сред;
- принципы разработки алгоритмов программ, основных приемов программирования;
- модели баз данных;
- принципы построения, физические основы работы периферийных устройств;
- теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;
- порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;

− принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля

Всего – 792 часов, в том числе:

- максимальная учебная нагрузка обучающегося – 792 часа, включая:
- обязательную аудиторную учебную нагрузку обучающегося – 672 часа;
- самостоятельную работу обучающегося – 106 часа;
- учебная и производственная практика – 288 часов;
- промежуточная аттестация – 18 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности: обеспечение проектной деятельности, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование видов деятельности и профессиональных компетенций
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
ПК 1.4	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА: ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды общих и профессиональных компетенций	**Наименования разделов профессионального модуля****	**Всего часов** (макс.учебная нагрузка и практика)	**Объем часов, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося:**		**Учебная, часов**	**Производственная (по профилю специальности),** часов (если предусмотрена рассредоточенная практика)
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,**	**в т.ч. курсовая работа (проект),** часов	**Всего,** часов	**в т.ч. курсовая работа (проект),** часов		
1	2	3	4	5	6	7	8	9	10
ПК 1.1 – ПК 1.4	Раздел 1. МДК.01.01 Операционные системы	**72**	**58**	28	-	**14**			**-**
	Раздел 2. МДК.01.02 Базы данных	**72**	**58**	28	-	**14**			**-**
	Раздел 3. МДК.01.03 Сети и системы передачи информации	**72**	**54**	18	-	**18**			
	Раздел 4. МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	**144**	**110**	40	-	**34**			
	Раздел 5. МДК.01.05 Эксплуатация компьютерных сетей	**126**	**100**	40		**26**			
	Учебная практика	**108**						**108**	
	Производственная практика (по профилю специальности), часов	**180**							**180**
	Экзамен по профессиональному модулю[1]	**18**							**-**
	Всего:	**792**	**672**	154	-	**106**		**108**	**180**

[1] Часы на экзамен по профессиональному модулю выделяются за счет вариативной части.

3.2. Тематический план и Содержание учебного материала: профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала: учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов
1	2	3
МДК.01.01 Операционные системы		**58**
	IV семестр	**58**
Раздел 1. Элементы теории операционных систем. Свойства операционных систем		**32**
Тема 1.1. Основы теории операционных систем	**Содержание учебного материала:** 1. Определение операционной системы. Основные понятия. История развития операционных систем. 2. Виды операционных систем. Классификация операционных систем по разным признакам. 3. Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.	2
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	**Содержание учебного материала:** 1. Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС. 2. Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. 3. Драйверы. Поддержка операций ввода-вывода. Работа с файлами. Файловая система. Виды файловых систем. 4. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.	4
	Практические занятия Практическая работа № 1 Виртуальные машины. Создание, модификация, работа Практическая работа № 2 Установка ОС Практическая работа № 3 Создание и изучение структуры разделов жесткого диска Практическая работа № 4 Операции с файлами	6

Тема 1.3. Модульная структура операционных систем, пространство пользователя	**Содержание учебного материала:** Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.	2
	Практические занятия Практическая работа № 5 Работа в консольном и графическом режимах	2
Тема 1.4. Управление памятью	**Содержание учебного материала:** Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти	4
	Практические занятия Практическая работа № 6 Мониторинг за использованием памяти	2
Тема 1.5. Управление процессами, многопроцессорные системы	**Содержание учебного материала:** 1. Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие 2. Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	2
	Практические занятия Практическая работа № 7 Управление процессами Практическая работа № 8 Наблюдение за использованием ресурсов системы	2
Тема 1.6. Виртуализация и облачные технологии	**Содержание учебного материала:** 1. Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования 2. Облачные технологии. Исследования в области виртуализации и облаков	4
	Практические занятия Практическая работа № 9 Изучение примеров виртуальных машин (VMware, VBox)	2
Раздел 2. Безопасность операционных систем		**6**
Тема 2.1. Принципы построения защиты информации в операционных	**Содержание учебного материала:** 1. Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. 2. Аутентификация, авторизация, аудит.	2

системах	**Практические занятия** Практическая работа № 10 Управление учетными записями пользователей и доступом к ресурсам Практическая работа № 11 Аудит событий системы Практическая работа № 12 Изучение штатных средств защиты информации в операционных системах	4
Раздел 3. Особенности работы в современных операционных системах		**20**
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	**Содержание учебного материала:** 1. Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX. 2. Операционные системы семейства Mac OS: особенности, преимущества и недостатки. 3. Архитектура Android. Приложения Android	6
	Практические занятия Практическая работа № 13 Создание дистрибъютива Linux. Установка. Практическая работа № 14 Работа в ОС Linux. Практическая работа № 15 Работа в ОС Linux.	4
Тема 3.2. Операционная система Windows	**Содержание учебного материала:** Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	2
	Практические занятия Практическая работа № 16 Установка и первичная настройка Windows.	2
Тема 3.3. Серверные операционные системы	**Содержание учебного материала:** Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы. Дифференцированный зачет.	2
	Практические занятия Практическая работа № 17 Работа с сетевой файловой системой. Практическая работа № 18 Работа с серверной ОС, например, AltLinux.	4
	Самостоятельная работа обучающегося: 1. Создание виртуальной машины. 2. Установка операционной системы.	14
МДК.01.02 Базы данных		**58**
Раздел 4. Основы теории баз данных		**9**

Тема 4.1. Основные понятия теории баз данных. Модели данных	**Содержание учебного материала:** Базы данных: понятие, компоненты, классификация.	2
Тема 4.2. Основы реляционной алгебры	**Содержание учебного материала:** Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	2
	Практические занятия Практическая работа № 1 Операции над отношениями	1
Тема 4.2. Базовые понятия и классификация систем управления базами данных	**Содержание учебного материала:** Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие.	2
Тема 4.3. Целостность данных как ключевое понятие баз данных	**Содержание учебного материала:** Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	2
Раздел 5. Проектирование баз данных		**9**
Тема 5.1. Информационные модели реляционных баз данных	**Содержание учебного материала:** Типы информационных моделей. Логические модели данных. Физические модели данных.	2
	Практические занятия Практическая работа № 2 Проектирование инфологической модели данных	1
Тема 5.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	**Содержание учебного материала:** Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам. Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.	2
	Практические занятия Практическая работа № 3 Проектирование структуры базы данных	1
Тема 5.3. Средства автоматизации	**Содержание учебного материала:** CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое	2

проектирования	представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	
	Практические занятия Практическая работа № 4 Проектирование базы данных с использованием CASE-средств	1
Раздел 6. Организация баз данных		**9**
Тема 6.1. Создание базы данных. Манипулирование данными.	**Содержание учебного материала:** Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.	2
	Практические занятия Практическая работа № 5 Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	1
Тема 6.2. Индексы. Связи между таблицами. Объединение таблиц	**Содержание учебного материала:** Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	2
	Практические занятия Практическая работа № 6 Создание взаимосвязей. Сортировка, поиск и фильтрация данных Практическая работа № 7 Способы объединения таблиц	4
Раздел 7. Управление базой данных с помощью SQL		**8**
Тема 7.1. Структурированный язык запросов SQL	**Содержание учебного материала:** Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	2
	Практические занятия Практическая работа № 8 Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL	1
Тема 7.2. Операторы и функции языка SQL	**Содержание учебного материала:** Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	1
	Практические занятия Практическая работа № 9 Создание и использование запросов. Группировка и агрегирование данных	4

	Практическая работа № 10 Коррелированные вложенные запросы. Создание в запросах вычисляемых полей. Использование условий	
Раздел 8. Организация распределённых баз данных		**9**
Тема 8.1. Архитектуры распределенных баз данных	**Содержание учебного материала:** Архитектуры клиент/сервер. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных.	1
	Практические занятия Практическая работа № 11 Управление доступом к объектам базы данных	1
Тема 8.2. Серверная часть распределенной базы данных	**Содержание учебного материала:** Планирование и развёртывание СУБД для работы с клиентскими приложениями	1
	Практические занятия Практическая работа № 12 Установка СУБД. Настройка компонентов СУБД.	1
Тема 8.3. Клиентская часть распределенной базы данных	**Содержание учебного материала:** Планирование приложений. Организация интерфейса с пользователем. Оптимизация производительности работы СУБД.	1
	Практические занятия Практическая работа № 13 Создание форм и отчетов Практическая работа № 14 Создание меню. Генерация, запуск. Практическая работа № 15 Профилирование запросов клиентских приложений.	4
Раздел 9. Администрирование и безопасность		**12**
Тема 9.1. Обеспечение целостности, достоверности и непротиворечивости данных.	**Содержание учебного материала:** Угрозы целостности СУБД. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера.	1
	Практические занятия Практическая работа № 16 Разработка хранимых процедур и триггеров	1
	Самостоятельная работа обучающегося: 1. Выполнение индивидуального задания по теме «Создание пользовательского приложения средствами СУБД». 2. Разбор синтаксиса хранимых процедур и триггеров.	14

Тема 9.2. Перехват исключительных ситуаций и обработка ошибок	**Содержание учебного материала:** Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	1
Тема 9.3. Механизмы защиты информации в системах управления базами данных	**Содержание учебного материала:** Средства идентификации и аутентификации. Общие сведения. Средства защиты информации в базах данных	1
	Практические занятия Практическая работа № 17 Управление правами доступа к базам данных	1
Тема 9.4. Копирование и перенос данных. Восстановление данных	**Содержание учебного материала:** Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Дифференцированный зачет.	1
	Практические занятия Практическая работа № 18 Аудит данных с помощью средств СУБД и триггеров Практическая работа № 19 Резервное копирование и восстановление баз данных Практическая работа № 20 Резервное копирование и восстановление баз данных	6
МДК.01.03 Сети и системы передачи информации		**54**
Раздел 1. Теория телекоммуникационных сетей		**20**
Тема 1.1. Основные понятия и определения	**Содержание учебного материала:** 1. Классификация систем связи. Сообщения и сигналы. 2. Виды электронных сигналов. Спектральное представление сигналов. 3. Параметры сигналов. Объем и информационная емкость сигнала.	4
Тема 1.2. Принципы передачи информации в сетях и системах связи	**Содержание учебного материала:** 1. Назначение и принципы организации сетей. Классификация сетей. 2. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	6
Тема 1.3. Типовые каналы передачи и их характеристики	**Содержание учебного материала:** 1. Канал передачи. Сетевой тракт, групповой канал передачи. 2. Аппаратура цифровых плезиохронных систем передачи. 3. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	6
	Практические занятия Практическая работа № 1 Расчет пропускной способности канала связи Практическая работа № 2 Расчет пропускной способности канала связи	4

Раздел 2. Сети передачи данных		**39**
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	**Содержание учебного материала:** 1. Структура и характеристики сетей. Способы коммутации и передачи данных. 2. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи. 3. Протоколы и интерфейсы управления каналами и сетью передачи данных.	6
	Практические занятия Практическая работа № 3 Расчет пропускной способности канала связи Практическая работа № 4 Расчет пропускной способности канала связи Практическая работа № 5 Расчет пропускной способности канала связи Практическая работа № 6 Расчет пропускной способности канала связи Практическая работа № 7 Расчет пропускной способности канала связи Практическая работа № 8 Расчет пропускной способности канала связи	10
Тема 2.2. Беспроводные системы передачи данных	**Содержание учебного материала:** 1. Беспроводные каналы связи. Беспроводные сети Wi-Fi. 2. Преимущества и область применения. Основные элементы беспроводных сетей. 3. Стандарты беспроводных сетей. Технология WIMAX	6
	Практические занятия Практическая работа № 9 Расчет пропускной способности канала связи Практическая работа № 10 Расчет пропускной способности канала связи	4
	Самостоятельная работа обучающегося: 1. Настройка Wi-Fi маршрутизатора 2. Изучение сетевых утилит 3. Конфигурирование сетевого интерфейса 4. Маршрутизация и управление потоками в сетях связи	18
Тема 2.3. Сотовые и спутниковые системы	**Содержание учебного материала:** 1. Принципы функционирования систем сотовой связи. 2. Стандарты GSM и CDMA. 3. Спутниковые системы передачи данных.	6
МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**110**
Раздел 3. Разработка защищенных автоматизированных (информационных) систем		**60**

Тема 3.1. Основы информационных систем как объекта защиты.	**Содержание учебного материала:** 1. Понятие автоматизированной (информационной) системы. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. 2. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. 3. Требования к АИС: гибкость, надежность, эффективность, безопасность. 4. Основные особенности современных проектов АИС. Электронный документооборот.	4
	Практические занятия Практическая работа № 1 Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании) Практическая работа № 2 Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	4
Тема 3.2. Жизненный цикл автоматизированных систем	**Содержание учебного материала:** 1. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС. 2. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. 3. Методологии проектирования. Организация работ, функции заказчиков и разработчиков. 4. Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.	6
	Практические занятия Практическая работа № 3 Разработка технического задания на проектирование автоматизированной системы Практическая работа № 4 Разработка технического задания на проектирование автоматизированной системы Практическая работа № 5 Разработка технического задания на проектирование автоматизированной системы	6

Тема 3.3. Угрозы безопасности информации в автоматизированных системах	**Содержание учебного материала:** 1. Потенциальные угрозы безопасности в автоматизированных системах. 2. Источники и объекты воздействия угроз безопасности информации. 3. Критерии классификации угроз. Методы оценки опасности угроз. 4. Банк данных угроз безопасности информации. Понятие уязвимости угрозы. Классификация уязвимостей.	6
	Практические занятия Практическая работа № 6 Разработка технического задания на проектирование автоматизированной системы Практическая работа № 7 Разработка технического задания на проектирование автоматизированной системы Практическая работа № 8 Разработка технического задания на проектирование автоматизированной системы Практическая работа № 9 Разработка технического задания на проектирование автоматизированной системы Практическая работа № 10 Разработка технического задания на проектирование автоматизированной системы	10
	Самостоятельная работа обучающегося: 1. Разработка концепции защиты автоматизированной (информационной) системы 2. Анализ банка данных угроз безопасности информации 3. Анализ журнала аудита ОС на рабочем месте	16
Тема 3.4. Основные меры защиты информации в автоматизированных системах	**Содержание учебного материала:** 1. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах. 2. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах. 3. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним. 4. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним.	6

Тема 3.5. Порядок эксплуатации АС в защищенном исполнении	**Содержание учебного материала:** 1. Идентификация и аутентификация субъектов доступа и объектов доступа. 2. Управление доступом субъектов доступа к объектам доступа. Ограничение программной среды. Защита машинных носителей информации 3. Регистрация событий безопасности. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ. 4. Обнаружение (предотвращение) вторжений. Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. 5. Обеспечение доступности информации. Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения. Защита технических средств. 6. Защита информационной системы, ее средств, систем связи и передачи данных. 7. Резервное копирование и восстановление данных. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	6
Тема 3.6. Защита информации в распределенных автоматизированных системах	**Содержание учебного материала:** 1. Механизмы и методы защиты информации в распределенных автоматизированных системах. 2. Архитектура механизмов защиты распределенных автоматизированных систем. 3. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	6
Тема 3.7. Особенности разработки информационных систем персональных данных	**Содержание учебного материала:** 1. Общие требования по защите персональных данных. 2. Состав и Содержание учебного материала: организационных и технических мер по защите информационных систем персональных данных. 3. Порядок выбора мер по обеспечению безопасности персональных данных. 4. Требования по защите персональных данных, в соответствии с уровнем защищенности. Обязательная контрольная работа (ОКР).	6

	Практические занятия Практическая работа № 11 Разработка технического задания на проектирование автоматизированной системы Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн. Практическая работа № 12 Разработка технического задания на проектирование автоматизированной системы Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн. Практическая работа № 13 Разработка технического задания на проектирование автоматизированной системы Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн. Практическая работа № 14 Разработка технического задания на проектирование автоматизированной системы Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	8
Раздел 4.Эксплуатация защищенных автоматизированных систем.		**50**
Тема 4.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	**Содержание учебного материала:** 1. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. 2. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. 3. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. 4. Порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	6
Тема 4.2. Администрирование автоматизированных систем	**Содержание учебного материала:** 1. Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. 2. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. 3. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	6
Тема 4.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	**Содержание учебного материала:** 1. Порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. 2. Общие обязанности администратора информационной безопасности автоматизированных систем. 3. Общие обязанности администратора информационной безопасности автоматизированных систем.	6

Тема 4.4. Защита от несанкционированного доступа к информации	**Содержание учебного материала:** 1. Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. 2. Организация работ по защите от НСД. 3. Классификация автоматизированных систем. Требования по защите информации от НСД для АС. 4. Требования защищенности СВТ от НСД к информации. 5. Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ.	6
Тема 4.5. СЗИ от НСД	**Содержание учебного материала:** 1. Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. 2. Общие принципы управления. Основные механизмы защиты. 3. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам. 4. Управление доступом и контроль печати конфиденциальной информации. 5. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. 6. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. 7. Управление грифами конфиденциальности. 8. Обеспечение целостности информационной системы и информации. Централизованное управление. системой защиты, оперативный мониторинг и аудит безопасности.	6
	Практические занятия Практическая работа № 15 Установка и настройка СЗИ от НСД Практическая работа № 16 Защита входа в систему (идентификация и аутентификация пользователей) Практическая работа № 17 Разграничение доступа к устройствам. Управление доступом.	8
Тема 4.6. Эксплуатация средств защиты информации в компьютерных сетях	**Содержание учебного материала:** 1. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях. 2. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении.	6

	Практические занятия Практическая работа № 18 Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	2
Тема 4.7. Документация на защищаемую автоматизированную систему	**Содержание учебного материала:** Основные эксплуатационные документы защищенных автоматизированных систем.	2
	Практические занятия Практическая работа № 19 Оформление основных эксплуатационных документов на автоматизированную систему.	2
	Самостоятельная работа обучающегося: 1. Построение сводной матрицы угроз автоматизированной (информационной) системы 2. Анализ политик безопасности информационного объекта 3. Изучение аналитических обзоров в области построения систем безопасности 4. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации	18
МДК.01.05. Эксплуатация компьютерных сетей		**100**
Раздел 5. Основы передачи данных в компьютерных сетях		**40**
Тема 5.1. Модели сетевого взаимодействия	**Содержание учебного материала:** 1. Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI. 2. Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	2
	Практические занятия Практическая работа № 1 Изучение элементов кабельной системы.	2

Тема 5.2. Физический уровень модели OSI	**Содержание учебного материала:** 1. Понятие линии и канала связи. Сигналы. Основные характеристики канала связи. 2. Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа. Оптоволоконные линии связи. 3. Стандарты кабелей. Электрическая проводка. 4. Беспроводная среда передачи.	2
	Практические занятия Практическая работа № 2 Создание сетевого кабеля на основе неэкранированной витой пары (UTP) Практическая работа № 3 Сварка оптического волокна	4
Тема 5.3. Топология компьютерных сетей	**Содержание учебного материала:** 1. Понятие топологии сети. Сетевое оборудование в топологии. 2. Обзор сетевых топологий**.**	2
	Практические занятия Практическая работа № 4 Разработка топологи сети небольшого предприятия Практическая работа № 5 Построение одноранговой сети	4
Тема 5.4. Технологии Ethernet	**Содержание учебного материала:** 1. Обзор технологий построения локальных сетей. 2. Технология Ethernet. Физический уровень. Технология Ethernet. Канальный уровень	2
	Практические занятия Практическая работа № 6 Изучение адресации канального уровня. MAC-адреса. Практическая работа № 7 Изучение адресации канального уровня. MAC-адреса.	4
Тема 5.5. Технологии коммутации	**Содержание учебного материала:** 1. Алгоритм прозрачного моста. Методы коммутации. 2. Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети. Технология PoweroverEthernet	2
	Практические занятия Практическая работа № 8 Создание коммутируемой сети Практическая работа № 9 Создание коммутируемой сети	4

Тема 5.6. Сетевой протокол IPv4	**Содержание учебного материала:** 1. Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов. 2. Маршрутизация пакетов IPv4. Протоколы динамической маршрутизации	2
	Практические занятия Практическая работа № 10 Изучение IP-адресации. Практическая работа № 11 Изучение IP-адресации.	4
Тема 5.7. Скоростные и беспроводные сети	**Содержание учебного материала:** 1. Сеть FDDI. Сеть 100VG-AnyLAN 2. Сверхвысокоскоростные сети. Беспроводные сети	2
	Практические занятия Практическая работа № 12 Настройка беспроводного сетевого оборудования Практическая работа № 13 Настройка беспроводного сетевого оборудования	4
Раздел 6. Технологии коммутации и маршрутизации современных сетей Ethernet		**44**
Тема 6.1. Основы коммутации	**Содержание учебного материала:** Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов.	2
Тема 6.2. Начальная настройка коммутатора	**Содержание учебного материала:** Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.	2
	Практические занятия Практическая работа № 14 Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов Практическая работа № 15 Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	2

Тема 6.3. Виртуальные локальные сети (VLAN)	**Содержание учебного материала:** Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP. Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation.	2
	Практические занятия Практическая работа № 16 Настройка VLAN на основе стандарта IEEE 802.1Q Практическая работа №17 Настройка протокола GVRP. Практическая работа № 18 Настройка сегментации трафика без использования VLAN. Настройка функции Q-in-Q (Double VLAN).	2
	Самостоятельная работа обучающегося: Создание ЛВС на основе стандарта IEEE 802.1Q.	12
Тема 6.4. Функции повышения надежности и производительности	**Содержание учебного материала:** Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP. Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol. Обязательная контрольная работа.	2
	Практические занятия Практическая работа № 19 Настройка протоколов связующего дерева STP, RSTP, MSTP.	2
Тема 6.5. Адресация сетевого уровня и маршрутизация	**Содержание учебного материала:** 1. Обзор адресации сетевого уровня. 2. Формирование подсетей. 3. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса. 4. Протокол IPv6. 5. Формирование идентификатора интерфейса. 6. Способы конфигурации IPv6-адреса. 7. Планирование подсетей IPv6. Протокол NDP. 8. Понятие маршрутизации. 9. Дистанционно-векторные протоколы маршрутизации. 10. Протокол RIP.	8
	Практические занятия Практическая работа № 20 Основные конфигурации маршрутизатора. Практическая работа № 21 Настройка функции защиты от образования петель LoopBackDetection. Агрегирование каналов. Расширенные конфигурации маршрутизатора.	4

	Практическая работа № 22 Работа с протоколом CDP. Работа с протоколом TELNET. Работа с протоколом TFTP. Работа с протоколом RIP. Работа с протоколом OSPF. Конфигурирование функции маршрутизатора NAT/PAT. Конфигурирование PPP и CHAP.	
Тема 6.6. Качество обслуживания (QoS)	**Содержание учебного материала:** 1. Модели QoS. 2. Приоритезация пакетов. 3. Классификация пакетов. 4. Маркировка пакетов. 5. Управление перегрузками и механизмы обслуживания очередей. 6. Механизм предотвращения перегрузок. 7. Контроль полосы пропускания. 8. Пример настройки QoS.	10
	Практические занятия Практическая работа № 23 Настройка QoS. Приоритизация трафика. Управление полосой пропускания	2
Тема 6.7. Функции обеспечения безопасности и ограничения доступа к сети	**Содержание учебного материала:** Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора. Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.	2
	Практические занятия Практическая работа № 24 Списки управления доступом (AccessControlList). Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.	2
Тема 6.8. Многоадресная рассылка	**Содержание учебного материала:** 1. Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки. 2. Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping).Функция IGMP FastLeave.	2
	Практические занятия Практическая работа № 25 Отслеживание трафика многоадресной рассылки. Отслеживание трафика Multicast	2

Тема 6.9. Функции управления коммутаторами	**Содержание учебного материала:** 1. Управление множеством коммутаторов. Протокол SNMP. 2. RMON (Remote Monitoring). Функция Port Mirroring.	2
	Практические занятия Практическая работа № 26 Функции анализа сетевого трафика. Настройка протокола управления топологией сети LLDP.	2
Раздел 7. Межсетевые экраны		**16**
Тема 7.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	**Содержание учебного материала:** 1. Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры. 2. Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. 3. Криптографические механизмы безопасности.	4
Тема 7.2. Межсетевые экраны	**Содержание учебного материала:** 1. Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT. 2. Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.	2
	Практические занятия Практическая работа № 27 Основы администрирования межсетевого экрана. Соединение двух локальных сетей межсетевыми экранами**.** Создание политики без проверки состояния.	2
Тема 7.3. Системы обнаружения и предотвращения проникновений	**Содержание учебного материала:** Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства. Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.	2
	Практические занятия Практическая работа № 28 Обнаружение и предотвращение вторжений.	2
Тема 7.4. Приоритизация трафика и создание альтернативных маршрутов	**Содержание учебного материала:** Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.	2
	Практические занятия Практическая работа № 29 Создание альтернативных маршрутов с использованием статической маршрутизации	2

	Самостоятельная работа обучающегося: 1. Физическое кодирование с использованием манчестерского кода 2. Логическое кодирование с использованием скремблирования 3. Подключение клиента к беспроводной сети в инфраструктурном режиме	14
Учебная практика раздела МДК. 01.03 - МДК 01.05. **Виды работ** 1. Проведение аудита защищенности автоматизированной системы. 2. Установка, настройка и эксплуатация сетевых операционных систем. 3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 4. Организация работ с удаленными хранилищами данных и базами данных. 5. Организация защищенной передачи данных в компьютерных сетях. 6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. 7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. 8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.		***108***
Производственная практика **Виды работ:** 1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения 3. Настройка программного обеспечения с соблюдением требований по защите информации 4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам 5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением 6. Настройка встроенных средств защиты информации программного обеспечения 7. Проверка функционирования встроенных средств защиты информации программного обеспечения 8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения 9. Обслуживание средств защиты информации в компьютерных системах и сетях 10. Обслуживание систем защиты информации в автоматизированных системах 11. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем 12. Проверка работоспособности системы защиты информации автоматизированной системы		***180***

13. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации 14. Контроль стабильности характеристик системы защиты информации автоматизированной системы 15. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем 16. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	
Экзамен по профессиональному модулю	**18**
Всего	**792**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к материально-техническому обеспечению

Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Класс компьютерного моделирования: парты, столы, стулья, компьютерные столы, интерактивная доска, компьютеры, в составе локальной вычислительной сети факультета, подключенной к интернет, сетевое оборудование.

Adobe Reader, Microsoft Office, SP3,Браузеры (Chrome, FireFox)

Лаборатория «Информационных технологий, программирования и баз данных»:

рабочие места на базе вычислительной техники по одному рабочему месту на обучающегося, подключенными к локальной вычислительной сети и сети «Интернет»;

программное обеспечение сетевого оборудования;

обучающее программное обеспечение.

Лаборатория «Сетей и систем передачи информации»:

типовые комплекты учебного оборудования «Телекоммуникационные линии связи», «Персональный компьютер», «Локальные компьютерные сети» LAN-C, «Глобальные компьютерные сети» WAN, «Сети сотовой связи GSM/3G/LTE», «Корпоративные компьютерные сети» CAN, «Сенсорные сети ZigBee».

3.2. Информационное обеспечение реализации программы

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

3.2.1 Электронные издания (электронные ресурсы)

Основные источники

1. Богатырев, В. А. Надежность информационных систем : учебное пособие для среднего профессионального образования / В. А. Богатырев. — Москва : Издательство Юрайт, 2023. — 318 с. — (Профессиональное образование). — ISBN 978-5-534-15205-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520442 (дата обращения: 30.06.2023).

2. Шишмарёв, В. Ю. Диагностика и надежность автоматизированных систем : учебник для среднего профессионального образования / В. Ю. Шишмарёв. — 2-е изд. — Москва : Издательство Юрайт, 2023. — 341 с. — (Профессиональное образование). — ISBN 978-5-534-13629-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/517988

3. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования / О. М. Замятина. — Москва : Издательство Юрайт, 2020. — 159 с. — (Профессиональное образование). — ISBN 978-5-534-10682-4. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456799

Дополнительные источники

1. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2023. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/517817

2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях : учебник и практикум для среднего профессионального образования / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 423 с. — (Профессиональное

образование). — ISBN 978-5-534-16551-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531278

3. Станкевич, Л. А. Интеллектуальные системы и технологии : учебник и практикум для среднего профессионального образования / Л. А. Станкевич. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 495 с. — (Профессиональное образование). — ISBN 978-5-534-16241-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530660

3.2.2. Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей; https://ichip.ru/
2. Журналы Защита информации. Инсайд: Информационно-методический журнал. http://www.inside-zi.ru/
3. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. http://cyberrus.com/
4. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. http://bit.mephi.ru/

3.2.3. Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Российский биометрический портал www.biometrics.ru
4. Сайт журнала Информационная безопасность http://www.itsec.ru
5. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
6. Федеральный портал «Информационно-коммуникационные технологии в образовании» http://window.edu.ru/
7. Федеральный портал «Российское образование» www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

РАБОЧАЯ ПРОГРАММА

учебной дисциплины
ПМ.03. ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ
для специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем
(базовая подготовка)
на базе основного общего образования

Рабочая программа разработана на основе требований Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Зарегистрировано в Минюсте России 09.12.2016 N 1553) (ред. от 17.12.2020)

Разработчик: преподаватель АНО ВО «Российский новый университет» Поляков А.Н.,
Протокол «102/168 от 28.08.2026»

СОДЕРЖАНИЕ

1	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2	РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
3	СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	8
4	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	21
5	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)	23

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля (далее – рабочая программа) является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности (специальностям) СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида профессиональной деятельности (ВПД) ПМ.03. Защита информации техническими средствами и соответствующих **профессиональных компетенций (ПК):**

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

ПРОИЗВОДСТВЕННАЯ (ПРЕДДИПЛОМНАЯ) ПРАКТИКА

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-
аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах
отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-
аппаратных средств защиты информации.

ПК 2.4.Осуществлять обработку, хранение и передачу информации ограниченного
доступа.

ПК 2.5.Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6.Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

ПК 4.1.Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного
обеспечения

ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами,
таблицами, презентациями и содержанием баз данных, работать в графических редакторах

ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и
сервисов Интернета

ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной
Системе.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

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

иметь практический опыт:

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;
- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;
- проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
- проведения измерений параметров фоновых шумов, а также физических

полей, создаваемых техническими средствами защиты информации;

− установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

уметь:

− применять технические средства для криптографической защиты информации конфиденциального характера;

− применять технические средства для уничтожения информации и носителей информации;

− применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническимисредствами;

− применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

− применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

− применять инженерно-технические средства физической защиты объектов информатизации

знать:

− порядок технического обслуживания технических средств защиты информации;

- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
- физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей итехнических каналов утечки информации;
- порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;
- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
- номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
- основные принципы действия и характеристики технических средств физической защиты;
- основные способы физической защиты объектов информатизации;
- номенклатуру применяемых средств физической защиты объектов информатизации.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля

Всего – 720 часов, в том числе:
- максимальная учебная нагрузка обучающегося – 720 часа, включая:
- обязательную аудиторную учебную нагрузку обучающегося – 588 часа;
- самостоятельную работу обучающегося – 102 часа;
- учебная и производственная практика – 216 часов;
- промежуточная аттестация – 18 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности: обеспечение проектной деятельности, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование видов деятельности и профессиональных компетенций
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды общих и профессиональных компетенций	**Наименования разделов профессионального модуля****	**Всего часов** (макс.учебная нагрузка и практика)	**Объем часов, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося:**		**Учебная, часов**	**Производственная (по профилю специальности),** часов (если предусмотрена рассредоточенная практика)
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч. курсовая работа (проект),**часов	**Всего,** часов	**в т.ч. курсовая работа (проект),**часов		
1	2	3	4	5	6	7	8	9	10
ПК 3.1 – ПК 3.5	Раздел 1. МДК.03.01 Техническая защита информации	**216**	**162**	78	-	**54**			**-**
	Раздел 2. МДК.03.02 Инженерно-технические средства физической защиты объектов информации	**270**	**206**	98	18	**48**			**-**
	Учебная практика	**72**						**72**	
	Производственная практика (по профилю специальности), часов	**144**							**144**
	Промежуточная аттестация МДК.03.01 [1]	**18**							**-**
	Всего:	**720**	**588**	176	18	**102**		**72**	**144**

[1] Выбор формы промежуточной аттестации в основных образовательных программах определяется образовательной организацией самостоятельно.

3.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
МДК.03.01 Техническая защита информации		**216**
Раздел 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание учебного материала:** 1. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные параметры системы защиты информации.	2
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание учебного материала:** 1. Задачи и требования к способам и средствам защиты информации техническими средствами. 2. Принципы системного анализа проблем инженерно-технической защиты информации. 3. Классификация способов и средств защиты информации.	6
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	**Содержание учебного материала:** 1. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. 2. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. 3. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	6
	Практические занятия Практическая работа № 1. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. Практическая работа № 2. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. Практическая работа № 3. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	8

	Самостоятельная работа обучающегося: Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	4
Тема 2.2. Технические каналы утечки информации	**Содержание учебного материала:** 1. Понятие и особенности утечки информации. Структура канала утечки информации. 2. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. 3.Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	6
	Практические занятия Практическая работа № 4. Угрозы информационной безопасности. Практическая работа № 5. Угрозы информационной безопасности. Практическая работа № 6. Угрозы информационной безопасности.	8
Тема 2.3. Методы и средства технической разведки	**Содержание учебного материала:** 1. Классификация технических средств разведки. Методы и средства технической разведки. 2.Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. 3.Средства дистанционного съема информации.	6
	Практические занятия Практическая работа № 7. Организация аттестации выделенного помещения по требованиям безопасности информации. Практическая работа № 8. Организация аттестации выделенного помещения по требованиям безопасности информации.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Раздел 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание учебного материала:** 1. Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. 2. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. 3. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. 4. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей.	6
	Практические занятия Практическая работа № 9. Измерение параметров физических полей. Практическая работа № 10. Измерение параметров физических полей.	8

	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание учебного материала:** 1. Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. 2. Экранирование. Зашумление.	6
	Практические занятия Практическая работа № 11. Защита аппаратуры от электромагнитных полей. Практическая работа № 12. Защита аппаратуры от электромагнитных полей. Практическая работа № 13. Защита аппаратуры от электромагнитных полей.	8
	Самостоятельная работа обучающегося: Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	4
Раздел 4. Системы защиты от утечки информации		
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание учебного материала:** 1. Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. 2. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу. ОКР	6
	Практические занятия Практическая работа № 14. Защита от утечки по акустическому каналу. Практическая работа № 15. Защита от утечки по акустическому каналу.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание учебного материала:** 1. Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. 2. Негласная запись информации на диктофоны. Системы защиты от диктофонов. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	6
	Практические занятия Практическая работа № 16. Системы защиты от утечки информации по проводному каналу. Практическая работа № 17. Системы защиты от утечки информации по проводному каналу.	8

Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание учебного материала:** 1. Электронные стетоскопы. Лазерные системы подслушивания. 2. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	6
	Практические занятия Практическая работа № 18. Защита от утечки по виброакустическому каналу. Практическая работа № 19. Защита от утечки по виброакустическому каналу.	8
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание учебного материала:** 1. Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. 2. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладках. 3. Системы защиты от утечки по электромагнитному каналу. 4. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	6
	Практические занятия Практическая работа № 20. Определение каналов утечки ПЭМИН. Практическая работа № 21. Определение каналов утечки ПЭМИН. Практическая работа № 22. Защита от утечки по цепям электропитания и заземления. Практическая работа № 23. Защита от утечки по цепям электропитания и заземления.	8
	Самостоятельная работа обучающегося: Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	4
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание учебного материала:** 1. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. 2. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	6
	Практические занятия Практическая работа № 24. Технические средства защиты информации в телефонных линиях. Практическая работа № 25. Технические средства защиты информации в телефонных линиях.	8

	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание учебного материала:** 1. Низкочастотное устройство съема информации. 2. Высокочастотное устройство съема информации. 3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	6
	Практические занятия Практическая работа № 26. Системы защиты от утечки информации по электросетевому каналу. Практическая работа № 27. Системы защиты от утечки информации по электросетевому каналу.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание учебного материала:** 1. Телевизионные системы наблюдения. Приборы ночного видения. 2. Системы защиты информации по оптическому каналу.	8
	Практические занятия Практическая работа № 28. Системы защиты от утечки информации по оптическому каналу	8
	Самостоятельная работа обучающегося: Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	4
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение технических средств защиты информации	**Содержание учебного материала:** 1. Технические средства для уничтожения информации и носителей информации, порядок применения. 2. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. 3. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. 4. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. 5. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	8
	Практические занятия Практическая работа № 29. Применение технических средств защиты информации. Практическая работа № 30. Применение технических средств защиты информации. Практическая работа № 31. Применение технических средств защиты информации.	8

	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание учебного материала:** 1. Этапы эксплуатации технических средств защиты информации. 2. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. 3. Установка и настройка технических средств защиты информации. 4. Установка и настройка технических средств защиты информации. 5. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. 6. Организация ремонта технических средств защиты информации. 7. Проведение аттестации объектов информатизации.	8
	Практические занятия Практическая работа № 32. Эксплуатация технических средств защиты информации. Практическая работа № 33. Эксплуатация технических средств защиты информации.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	4
Промежуточная аттестация по МДК.03.01 в форме экзамена		**18**
Учебная практика по МДК.03.01 **Виды работ:** ~ Измерение параметров физических полей. ~ Определение каналов утечки ПЭМИН. ~ Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. ~ Установка и настройка технических средств защиты информации. ~ Проведение измерений параметров побочных электромагнитных излучений и наводок. ~ Проведение аттестации объектов информатизации.		
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**270**
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание учебного материала:** 1. Характеристики потенциально опасных объектов. 2. Содержание и задачи физической защиты объектов информатизации. 3. Содержание и задачи физической защиты объектов информатизации. 4. Основные понятия инженерно-технических средств физической защиты. 5. Основные понятия инженерно-технических средств физической защиты. 6. Категорирование объектов информатизации. 7. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.	10

	8. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. 9. Особенности задач охраны различных типов объектов. 10. Особенности задач охраны различных типов объектов.	
	Тематика практических занятий и лабораторных работ Практическая работа № 1. Характеристика объекта защиты. Практическая работа № 2. Характеристика объекта защиты. Практическая работа № 3. Характеристика объекта защиты.	8
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание учебного материала:** 1. Общие принципы обеспечения безопасности объектов. 2. Жизненный цикл системы физической защиты. 3. Жизненный цикл системы физической защиты. 4. Принципы построения интегрированных систем охраны. 5. Принципы построения интегрированных систем охраны. 6. Классификация и состав интегрированных систем охраны. 7. Классификация и состав интегрированных систем охраны. 8. Требования к инженерным средствам физической защиты. 9. Требования к инженерным средствам физической защиты. 10. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. 11. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	10
	Практические занятия Практическая работа № 4. Анализ нормативно-правовой базы физической защиты. Практическая работа № 5. Анализ нормативно-правовой базы физической защиты. Практическая работа № 6. Анализ нормативно-правовой базы физической защиты. Практическая работа № 7. Формирование требований к физической защите объекта. Практическая работа № 8. Формирование требований к физической защите объекта. Практическая работа № 9. Формирование требований к физической защите объекта	10
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	6
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание учебного материала:** 1. Информационные основы построения системы охранной сигнализации. 2. Информационные основы построения системы охранной сигнализации. 3. Назначение, классификация технических средств обнаружения. 4. Назначение, классификация технических средств обнаружения.	10

	5. Построение систем обеспечения безопасности объекта. 6. Построение систем обеспечения безопасности объекта. 7. Построение систем обеспечения безопасности объекта. 8. Периметровые средства обнаружения: назначение, устройство, принцип действия. 9. Периметровые средства обнаружения: назначение, устройство, принцип действия. 10. Периметровые средства обнаружения: назначение, устройство, принцип действия. 11. Объектовые средства обнаружения: назначение, устройство, принцип действия. 12. Объектовые средства обнаружения: назначение, устройство, принцип действия. ОКР.	
	Практические занятия Практическая работа № 10. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 11. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 12. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 13. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 14. Монтаж датчиков пожарной и охранной сигнализации. Практическая работа № 15. Монтаж датчиков пожарной и охранной сигнализации.	10
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	6
Тема 2.2. Система контроля и управления доступом	**Содержание учебного материала:** 1. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. 2. Особенности построения и размещения СКУД. 3. Структура и состав СКУД. 4. Периферийное оборудование и носители информации в СКУД. 5. Основы построения и принципы функционирования СКУД. 6. Классификация средств управления доступом. 7. Средства идентификации и аутентификации. 8. Методы удостоверения личности, применяемые в СКУД. 9. Методы удостоверения личности, применяемые в СКУД. 10. Обнаружение металлических предметов и радиоактивных веществ.	10
	Практические занятия Практическая работа № 16. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя. Практическая работа № 17. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя Практическая работа № 18. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя.	10

	Практическая работа № 19. Рассмотрение принципов устройства, работы и применения средств контроля доступа. Практическая работа № 20. Рассмотрение принципов устройства, работы и применения средств контроля доступа.	
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Тема 2.3. Система телевизионного наблюдения	**Содержание учебного материала:** 1. Аналоговые и цифровые системы видеонаблюдения. 2. Назначение системы телевизионного наблюдения. 3. Состав системы телевизионного наблюдения. 4. Видеокамеры. 5. Объективы. 6. Термокожухи. 7. Поворотные системы. 8. Инфракрасные осветители. 9. Детекторы движения.	8
	Практические занятия Практическая работа № 21. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. Практическая работа № 22. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. Практическая работа № 23. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. Практическая работа № 24. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	10
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание учебного материала:** 1. Классификация системы сбора и обработки информации. 2. Классификация системы сбора и обработки информации. 3. Схема функционирования системы сбора и обработки информации. 4. Схема функционирования системы сбора и обработки информации.	8

	5. Варианты структур построения системы сбора и обработки информации. 6. Варианты структур построения системы сбора и обработки информации. 7. Устройства отображения и документирования информации.	
	Практические занятия Практическая работа № 25. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. Практическая работа № 26. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. Практическая работа № 27. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. Практическая работа № 28. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	10
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Тема 2.5 Система воздействия	**Содержание учебного материала:** 1. Назначение и классификация технических средств воздействия. 2. Назначение и классификация технических средств воздействия. 3. Основные показатели технических средств воздействия. 4. Основные показатели технических средств воздействия.	10
	Практические занятия Практическая работа № 29. Выбор и обоснование средств подсистемы задержки. Практическая работа № 30. Выбор и обоснование средств подсистемы задержки. Практическая работа № 31. Выбор и обоснование средств подсистемы задержки.	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		**73**

Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание учебного материала:** 1. Периметровые и объектовые средства обнаружения, порядок применения. 2. Работа с периферийным оборудованием системы контроля и управления доступом. 3. Особенности организации пропускного режима на КПП. 4. Управление системой телевизионного наблюдения с автоматизированного рабочего места. 5. Порядок применения устройств отображения и документирования информации. 6. Управление системой воздействия. ОКР.	10
	Практические занятия Практическая работа № 32. Разработка структурной схемы и спецификации оборудования Практическая работа № 33. Разработка структурной схемы и спецификации оборудования Практическая работа № 34. Разработка структурной схемы и спецификации оборудования Практическая работа № 35. Разработка структурной схемы и спецификации оборудования	8
	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	6
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание учебного материала:** 1. Этапы эксплуатации. 2. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. 3. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. 4. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. 5. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. 6. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. 7. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. 8. Организация ремонта технических средств физической защиты. Дифференцированный зачет.	10
	Практические занятия Практическая работа № 36. Эксплуатация инженерно-технических средств физической защиты. Практическая работа № 37. Эксплуатация инженерно-технических средств физической защиты Практическая работа № 38. Эксплуатация инженерно-технических средств физической защиты Практическая работа № 39. Эксплуатация инженерно-технических средств физической защиты Практическая работа № 40. Эксплуатация инженерно-технических средств физической защиты	10

	Самостоятельная работа обучающегося: Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	6
Обязательная аудиторная учебная нагрузка по курсовой работе		**18**
Примерная тематика курсовых работ: 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества. 4. Основные операции проведения технического обслуживания инженерно-технических средств физической защиты. 5. Размещение периметровых средств обнаружения на местности.		
Учебная практика по разделу по МДК.03.02 1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации.		***72***
Производственная практика профессионального модуля ПМ.03 **Виды работ** 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.		***144***
Экзамен по профессиональному модулю		***18***
Всего		***720***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к материально-техническому обеспечению

Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Компьютерные классы: парты, столы, стулья, компьютерные столы, интерактивная доска, компьютеры, в составе локальной вычислительной сети факультета, подключенной к интернет, сетевое оборудование.

Adobe Reader, Microsoft Office, SP3,Браузеры (Chrome, FireFox)

Лаборатория «Технических, программных и программно-аппаратных средств защиты информации»

Лабораторный стенд «Защита информации от утечек по акустовибрационным каналам», Типовой комплект учебного оборудования
«Сетевая безопасность» SECURITY.

3.2. Информационное обеспечение реализации программы

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

3.2.1 Электронные издания (электронные ресурсы) Основные источники

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023.
— 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518006.

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519364

3. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519614

Дополнительные источники

1. Толстобров, А. П. Архитектура ЭВМ : учебное пособие для среднего профессионального образования / А. П. Толстобров. — 2-е изд., испр. идоп. — М.: Издательство Юрайт, 2021. — 154 с. — (Профессиональное

образование). — ISBN 978-5-534-13398-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/476555

2. Новожилов, О. П. Архитектура компьютерных систем в 2 ч. Часть1

: учебное пособие для среднего профессионального образования / О. П. Новожилов. — М.: Издательство Юрайт, 2021. — 276 с. — (Профессиональное образование). — ISBN 978-5-534-10299-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/475573

3. Новожилов, О. П. Архитектура компьютерных систем в 2 ч. Часть2

: учебное пособие для среднего профессионального образования / О. П. Новожилов. — М.: Издательство Юрайт, 2021. — 246 с. — (Профессиональное образование). — ISBN 978-5-534-10301-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/475574

3.2.2. Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей; https://ichip.ru/
2. Журналы Защита информации. Инсайд: Информационно-методический журнал. http://www.inside-zi.ru/
3. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. http://cyberrus.com/
4. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. http://bit.mephi.ru/

3.2.3. Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Российский биометрический портал www.biometrics.ru
4. Сайт журнала Информационная безопасность http://www.itsec.ru
5. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
6. Федеральный портал «Информационно-коммуникационные технологии в образовании» http://window.edu.ru/

7. Федеральный портал «Российское образование» www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ,

(ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	техническими средствами обработки информации ограниченного доступа	экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов

		выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике