ПРИЛОЖЕНИЕ 1.1.1
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ (УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ)

Индекс УП/ПП	**ПМ** (индекс, наименование)	**Вид практики (учебная/ производственная**	**Тип (этап) практики** (при наличии)	**Семестр**	**Объем в часах**
УП. 01	ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Учебная практика		4-5	108
УП. 02	ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Учебная практика		7	72
УП 03	ПМ 03 Защита информации техническими средствами	Учебная практика		6	36
УП 04	ПМ 04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"	Учебная практика		4	108
УП 05.01	ПМ 05 Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30	Учебная практика		7	72

	килограммов и менее)"				
УП 06.01	ПМ 06 Интеграция облачных технологий в цифровую экономику	Учебная практика		6-7	144
		Всего УП	X	X	540
ПП. 01	ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Производственная практика		6	180
ПП. 02	ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Производственная практика		7	144
ПП. 03	ПМ 03 Защита информации техническими средствами			7	144
ПП 04.01	ПМ 04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"			4	108
ПП 06.01	ПМ 06 Интеграция облачных технологий в цифровую экономику			7	108
		Всего ПП	X	X	684
		Итого практики	X	X	1224

2025 г.

ПРИЛОЖЕНИЕ 1.1.1
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

УП.01 ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

УП.02 ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

УП.03 ПМ 03 Защита информации техническими средствами

УП 04 ПМ 04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"

УП 05.01 ПМ 05 Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)"

УП 06.01 ПМ 06 Интеграция облачных технологий в цифровую экономику

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Цель и место учебной практики в структуре образовательной программы:

Рабочая программа учебной практики является частью программы подготовки ППССЗ в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и реализуется в профессиональном цикле после прохождения междисциплинарных курсов (МДК) в рамках профессиональных модулей в соответствии с учебным планом (п. 5.1. ОПОП-П):

УП 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	МДК 01.01 Операционные системы МДК 01.02 Базы данных МДК 01.03 Сети и системы передачи данных МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении МДК 01.05 Эксплуатация компьютерных сетей
УП 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	МДК 02.01 Программные и программно-аппаратные средства защиты информации МДК 02.02 Криптографические средства защиты информации
УП 03 Защита информации техническими средствами	ПМ 03 Защита информации техническими средствами	МДК 03.01 Техническая защита информации МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации
УП 04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"	ПМ 04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"	МДК 04.01 Технология создания и обработки цифровой информации
УП 05.01 Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)"	ПМ 05 Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)"	МДК 05.01 Пилотирование беспилотных авиационных систем МДК 05.02 Программирование беспилотных авиационных систем
УП 06.01 Интеграция облачных технологий в цифровую экономику	ПМ 06 Интеграция облачных технологий в цифровую экономику	МДК 06.01 Квантовая защита данных

		МДК 06.02 Облачная кибербезопасность

Учебная практика направлена на развитие общих (ОК) и профессиональных компетенций (ПК):

Код ОК / ПК	**Наименование ОК / ПК**
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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	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.
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 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, 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.
ПК 4.1	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.2.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК. 5.1	Организовывать и осуществлять предварительную и предполетную подготовку беспилотных воздушных судов смешанного типа
ПК 5.2	Организовывать и осуществлять эксплуатацию беспилотных воздушных судов смешанного типа, в том числе в особых условиях и особых случаях в полете
ПК 6.1	Сборка и настройка систем квантового распределения ключа
ПК 6.2	Осуществлять подбор соответствующих оптических элементов
ПК 6.3	Выполнять работы по анализу источников ошибок
ПК 6.4	Выполнение работ по реализации связки классической и квантовой систем
ПК 6.5	Применение программных средств обеспечения безопасности информации веб приложений
ПК 6.6	*Обработка запросов заказчика в службе технической поддержки в соответствии с трудовым заданием*

Цель учебной практики: формирование первоначальных практических профессиональных умений в рамках профессиональных модулей данной ОПОП-П по видам деятельности: «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении», «Защита информации в автоматизированных системах программными и программно-аппаратными средствами», «Защита информации техническими средствами», «Выполнение работ по профессии «Оператор электронно-вычислительных и вычислительных машин»», «Выполнение работ по профессии 25331 "Оператор беспилотных

авиационных систем (с максимальной взлетной массой 30 килограммов и менее)», «Интеграция облачных технологий в цифровую экономику».

1.2. Планируемые результаты освоения учебной практики

В результате прохождения учебной практики по видам деятельности, предусмотренным ФГОС СПО и запросам работодателей, обучающийся должен получить практический опыт (сформировать умения):

Наименование вида деятельности	Практический опыт / умения
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Практический опыт установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем; администрирование автоматизированных систем в защищенном исполнении; эксплуатация компонентов систем защиты информации автоматизированных систем; диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении; Умения осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; обеспечивать работоспособность, обнаруживать и устранять неисправности;
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Практический опыт установка, настройка программных средств защиты информации в автоматизированной систем; обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети;

	тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации; решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности; работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе; Умения устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; применять средства гарантированного уничтожения информации; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; 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;
Защита информации техническими средствами	Практический опыт установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации; применение основных типов технических средств защиты информации; выявление технических каналов утечки информации;

	участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; проведение 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; проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации; установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты; Умения применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных 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 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.
Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"	Практический опыт Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах; Установка программно-аппаратных средств защиты информации Настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам; Умения

	Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации; Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации;
Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)»	Практический опыт Изучение полетного задания, отработка порядка его выполнения и действий при управлении беспилотным воздушным судном с максимальной взлетной массой 30 килограммов и менее Подбор и подготовка картографического материала Ознакомление с ограничениями в районе выполнения полета по маршруту (трассе); Ведение полетной и технической документации, в том числе в электронном виде с использованием сервисов цифрового журналирования операций; Умения Читать аэронавигационные материалы Анализировать метеорологическую, орнитологическую и аэронавигационную обстановку Использовать специализированные цифровые платформы полетно-информационного обслуживания и сервисы цифрового журналирования операций; Оценивать техническое состояние и готовность к использованию беспилотных авиационных систем Оформлять полетную и техническую документацию;
Интеграция облачных технологий в цифровую экономику	Практический опыт Монтаж оборудования систем Первичная настройка и проверка функционирования систем Монтаж программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД; Установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты систем от НД Первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД; Текущий, в том числе автоматизированный, контроль функционирования систем с установленными показателями Текущий, в том числе автоматизированный, контроль функционирования с установленными показателями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях; Восстановление процесса функционирования после сбоев и отказов систем, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях; составления базы знаний технической поддержки на основе обрабатываемых прецедентов; *Работы с оборудованием КРК; анализа и оценки угроз в квантовых коммуникациях; разработки и реализации решений по квантовой защите данных*

	Умения Проводить монтаж (для программных средств - установку) систем, средств и систем защиты систем от НД Проводить первичную настройку и проверку функционирования систем, средств и систем защиты систем от НД; Проводить проверку комплектности систем, средств и систем защиты систем от НД; Проводить текущий контроль показателей и процесса функционирования систем, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях электросвязи, предусмотренный регламентом их эксплуатации; Проводить предусмотренные регламентом работы по восстановлению процесса и параметров функционирования систем, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях; выяснять из беседы с заказчиком и понимать причины возникших аварийных ситуаций с информационным ресурсом; применять установленные правила делового общения при общении с заказчиком; отвечать на запросы заказчика в установленные регламентом сроки; анализировать и решать типовые запросы заказчиков; работать с программным обеспечением по приему, обработке и регистрации запросов заказчика; координировать решение запросов заказчиков со специалистами соответствующих подразделений; объяснять заказчикам пути решения возникшей проблемы; *Настраивать и эксплуатировать оборудование КРК; оценивать безопасность и стойкость систем квантовой криптографии; интегрировать КРК с существующими криптографическими системами;*

1.3. Обоснование часов учебной практики в рамках вариативной части ОПОП-П

УП	Код ПК/ дополнительные (ПК*, ПКц)	Практический опыт	Наименование темы практики	Объем часов	Обоснование увеличения объема практики
УП 01	ПК 1.5 Проектировать локальные компьютерные сети ПК 1.6 Проектировать виртуальные	проектирования локальных сетей; проектирования виртуальных компьютерных сетей; Выполнять работы с документами	Тема 1.3. Топологии компьютерных сетей Тема 2.3. Виртуальные локальные	108	по запросу работодателя

	компьютерные сети ПК 1.7 Проектировать реляционные базы данных ПК 1.8 Проектировать сети передачи данных ПК 1.9 Пользоваться нормативно-технической документацией в области защиты информации	отраслевой направленности; выполнения работ по проектированию сетей передачи данных; делать выбор средств защиты автоматизированных систем;	сети (VLAN) Раздел 5. Организация распределённых баз данных Тема 2.1. Архитектура и принципы работы современных сетей передачи данных Раздел 2.Эксплуатация защищенных автоматизированных систем		
УП 02	ПК 2.7. Производить анализ угроз и уязвимостей автоматизированных систем ПК 2.8. Разработка и внедрение мер защиты информации в автоматизированных системах	выявлять и оценивать потенциальные угрозы и уязвимости в автоматизированных системах, основываясь на анализе архитектуры и компонентов системы; проектировать системы защиты информации с учетом требований безопасности и особенностей автоматизированных систем.	Тема 1.3 Тема 1.9 Тема 2.1 Тема 2.5	72	по запросу работодателя
УП 05.01	ПК 5.1. Организовывать и осуществлять предварительную и	Изучение полетного задания, отработка порядка его выполнения и действий при управлении	Раздел 1. Пилотирование беспилотных	72	по запросу работодателя

	предполетную подготовку беспилотных воздушных судов смешанного типаслучаях в полете ПК 5.2. Организовывать и осуществлять эксплуатацию беспилотных воздушных судов вертолетного типа, в том числе в особых условиях и особых случаях в полете.	беспилотным воздушным судном с максимальной взлетной массой 30 килограммов и менее Подбор и подготовка картографического материала Ознакомление с ограничениями в районе выполнения полета по маршруту (трассе); владеть методами и алгоритмами инструментального и программного обеспечения систем автоматизации и управления;	авиационных систем Раздел 2. Программирование беспилотных авиационных систем		
УП 06.01	Вариативной части нет в пм			144	по запросу работодателя
Всего академических часов учебной практики в рамках вариативной части ОПОП-П - 396					

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

2.1. Трудоемкость освоения учебной практики

Код УП	Объем, ак.ч.	Форма проведения учебной практики (концентрированно/ рассредоточено)	Курс / семестр	Форма промежуточной аттестации
УП. 01	108	концентрированно	2-3/4-5	-
УП. 02	72	концентрированно	4/7	-
УП 03	36	концентрированно	3/6	-
УП 04	108	концентрированно	2/4	-
УП 05.01	72	концентрированно	4/7	-
УП 06.01	144	концентрированно	3-4/6-7	-
Всего УП	540	X	X	X

2.2. Структура учебной практики

Код ПК	Наименование разделов профессионального модуля	Виды работ	Наименование тем учебной практики	Объем часов
УП 01. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении				108
ПК 1.1 ПК 1.2. ПК 1.3 ПК 1.4	Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении МДК.01.01 Операционные системы	1. Проведение инструктажа по технике безопасности.	Тема 1.1. Основы теории операционных систем	1
			Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	1
			Тема 1.3. Модульная структура операционных систем, пространство пользователя	1
			Тема 1.4. Управление памятью	1
			Тема 1.5. Управление процессами, многопроцес	1

			сорные системы	
			Тема 1.6. Виртуализация и облачные технологии	2
			ВСЕГО ПО РАЗДЕЛУ 1	7
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4	Раздел 2. Безопасность операционных систем	1. Ознакомление с планом проведения учебной практики. Получение заданий по тематике.	Тема 2.1. Принципы построения защиты информации в операционных системах	7
			ВСЕГО ПО РАЗДЕЛУ 2	7
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4	Раздел 3. Особенности работы в современных операционных системах	Установка программного комплекса Secret Net на рабочие компьютеры пользователей. Базовая настройка.	Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	3
			Тема 3.2. Операционная система Windows	3
			Тема 3.3. Серверные операционные системы	1
			ВСЕГО ПО РАЗДЕЛУ 3	7
!!!	Раздел 1. Основы теории баз данных МДК.01.02 Базы данных	Настройка параметров работы программного обеспечения, включая системы управления базами данных (Установка Windows Server 2019 доменных служб AD. Настройка DNS)	Тема 1.1. Основные понятия теории баз данных. Модели данных	1
			Тема 1.2. Основы реляционной алгебры	1

			Тема 1.3. Базовые понятия и классификация систем управления базами данных	1
			Тема 1.4. Целостность данных как ключевое понятие баз данных	1
ВСЕГО ПО РАЗДЕЛУ 1				4
!!	Раздел 2. Проектирование баз данных	Создание учетных записей пользователей в домене. Настройка разграничений доступа.	Тема 2.1. Информационные модели реляционных баз данных	1
			Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	1
			Тема 2.3. Средства автоматизации проектирования	1
ВСЕГО ПО РАЗДЕЛУ 2				3

	Раздел 3. Организация баз данных	Установка сервера базы данных SQL и Postgresql. Установка SNS, создание политик.	Тема 3.1. Создание базы данных. Манипулирование данными.	2
			Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	2
			ВСЕГО ПО РАЗДЕЛУ 3	4
!!	Раздел 4. Управление базой данных с помощью SQL	Изучение, установка и настройка ПАК «Соболь». Инициализация, создание пользователей и назначение ключей. Объединение работы «Соболь» и SNS.	Тема 4.1. Структурированный язык запросов SQL	2
			Тема 4.2. Операторы и функции языка SQL	1
			ВСЕГО ПО РАЗДЕЛУ 4	3
!!	Раздел 5. Организация распределённых баз данных	Работа с «Соболь» с версии 3.0. Сравнительный анализ ПАК «Соболь» версии 3.0 и 4.0. Перепрошивка «Соболь» до версии 4.0.	Тема 5.1. Архитектуры распределенных баз данных	1
			Тема 5.2. Серверная часть распределенной базы данных	1

			Тема 5.3. Клиентская часть распределенной базы данных	1
			ВСЕГО ПО РАЗДЕЛУ 5	3
!!	Раздел 6. Администрирование и безопасность	Настройка контроля целостности операционной систем Windows 10 с применением ПАК «Соболь» версии 4.0	Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	1
			Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	1
			Тема 6.3. Механизмы защиты информации в системах управления базами данных	1
			Тема 6.4. Копирование и перенос данных. Восстановление данных	1
			ВСЕГО ПО РАЗДЕЛУ 6	4
!!	Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении МДК.01.03 Сети и системы передачи информации	Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных	Тема 1.1. Основные понятия и определения	3

			Тема 1.2. Принципы передачи информации в сетях и системах связи	3
			Тема 1.3. Типовые каналы передачи и их характеристики	5
ВСЕГО ПО РАЗДЕЛУ 2				11
	Раздел 2. Сети передачи данных	Настройка средств архивации данных Windows Server 2019	Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	5
			Тема 2.2. Беспроводные системы передачи данных	3
			Тема 2.3. Сотовые и спутниковые системы	2
ВСЕГО ПО РАЗДЕЛУ 2				10
	Раздел 1. Разработка защищенных автоматизированных (информационных) систем МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Проведение аудита защищенности автоматизированной системы	Тема 1.1. Основы информационных систем как объекта защиты.	2
			Тема 1.2. Жизненный цикл автоматизированных систем	1

			Тема 1.3. Угрозы безопасности информации в автоматизированных системах	1
			Тема 1.4. Основные меры защиты информации в автоматизированных системах	1
			Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	1
			Тема 1.6. Защита информации в распределенных автоматизированных системах	2
			Тема 1.7. Особенности разработки информационных систем персональных данных	2
			ВСЕГО ПО РАЗДЕЛУ 1	10
	Раздел 2. Эксплуатация защищенных автоматизированных систем.	Установка, настройка и эксплуатация Ubuntu Server и Ubuntu Desktop.	Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	1

			Тема 2.2. Администрирование автоматизированных систем	1
			Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	1
			Тема 2.4. Защита от несанкционированного доступа к информации	1
			Тема 2.5. СЗИ от НСД	1
			Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	1
			Тема 2.7. Документация на защищаемую автоматизированную систему	5
			ВСЕГО ПО РАЗДЕЛУ 2	11

	Раздел 1. Основы передачи данных в компьютерных сетях МДК.01.05. Эксплуатация компьютерных сетей	Настройка разграничения доступа штатными средствами Ubuntu.	Тема 1.1. Модели сетевого взаимодействия	1
			Тема 1.2. Физический уровень модели OSI	1
			Тема 1.3. Топология компьютерных сетей	1
			Тема 1.4. Технологии Ethernet	1
			Тема 1.5. Технологии коммутации	1
			Тема 1.6. Сетевой протокол IPv4	1
			Тема 1.7. Скоростные и беспроводные сети	1
			ВСЕГО ПО РАЗДЕЛУ 1	7
	Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet	Организация работ с удаленными хранилищами данных и базами данных.	Тема 2.1. Основы коммутации	2
			Тема 2.2. Начальная настройка коммутатора	2
			Тема 2.3. Виртуальные локальные сети (VLAN)	2
			Тема 2.4. Функции повышения надежности и производительности	2

			Тема 2.5. Адресация сетевого уровня и маршрутизация	2
			Тема 2.6. Качество обслуживания (QoS)	2
			Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	1
			Тема 2.8. Многоадресная рассылка	1
			Тема 2.9. Функции управления коммутаторами	1
			ВСЕГО ПО РАЗДЕЛУ 2	15
	Раздел 3. Межсетевые экраны	Работа в VMware ESXI. Установка виртуальных машин. . Настройка сети, поднятие сетевой инфраструктуры. Vlan. Поднятие l2tp туннеля на Mikrotik RouterOS Работа с Netstat, Nmap и Wireshark. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев в её работе. Составление многоуровневой схемы топологии созданной сети. Заполнение отчетной документации по техническому обслуживанию и	Тема 3.1. Межсетевые экраны	2

		ремонту компьютерных сетей. Оформление отчета. Участие в зачет-конференции по учебной практике		
			ВСЕГО ПО РАЗДЕЛУ 3	2
УП 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами				72
ПК 2.1 ПК 2.2 ПК 2.3 ПК.2.4 ПК 2.5 ПК.2.6	Раздел 1 Программные и программно-аппаратные средства защиты информации	1. Вводное занятие. Инструктаж по технике безопасности. 2. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах 3. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности 4. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности 5. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации 6. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	2
			Тема 1.2. Стандарты безопасности	2
			Тема 1.3. Защищенная автоматизированная система	2
			Тема 1.4. Дестабилизирующее воздействие на объекты защиты	2
			Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	2
			Тема 1.6 Основы защиты автономных автоматизированных систем	2
			Тема 1.7 Защита	2

			программ от изучения Тема 1.8 Вредоносное программное обеспечение	
			Тема 1.9 Защита программ и данных от несанкциони рованного копирования	2
			Тема 1.10 Защита информации на машинных носителях	2
			Тема 1.11. Системы обнаружения атак и вторжений	2
			Тема 1.12 Основы построения защищенных сетей	2
			Тема 1.13 Средства организации VPN	2
			Тема 1.14 Обеспечение безопасности межсетевого взаимодейст вия	2
			Тема 1.15 Мониторинг систем защиты	2
			Тема 1.16 Изучение мер защиты информации в информацио	2

			нных системах	
			ВСЕГО ПО РАЗДЕЛУ 1	36
ПК 2.1 ПК 2.2 ПК 2.3 ПК.2.4 ПК 2.5 ПК.2.6	Раздел 2. Криптографические средства защиты информации	1. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. 2. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. 3. Применение математических методов для оценки качества и выбора наилучшего программного средства 4. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи 5. Оформление отчета. Участие в зачет-конференции по учебной практике	Тема 2.1. Введение в криптографию	3
			Тема 2.2. Методы криптографического защиты информации	3
			Тема 2.3. Криптоанализ	3
			Тема 2.4. Поточные шифры и генераторы псевдослучайных чисел	3
			Тема 2.5 Кодирование информации. Компьютеризация шифрования.	3
			Тема 2.6 Симметричные системы шифрования	3
			Тема 2.7 Асимметричные системы шифрования	2
			Тема 2.8 Аутентификация данных. Электронная подпись	2
			Тема 2.9 Алгоритмы обмена ключей и протоколы аутентификации	2
			Тема 2.10	2

			Криптозащита информации в сетях передачи данных	
			Тема 2.11 Защита информации в электронных платежных системах	5
			Тема 2.12 Компьютерная стеганография	5
ВСЕГО ПО РАЗДЕЛУ 2				36
УП 03 Защита информации техническими средствами				36
ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4 ПК 3.5	Раздел 1. Техническая защита информации	1. Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике 2. Разработка организационных и технических мероприятий по заданию преподавателя; 3. Разработка основной документации по инженерно-технической защите информации.	Тема 1.1 Технические каналы утечки информации	9
			Тема 1.2. Способы и средства защиты информации по техническим каналам утечки информации	9
ВСЕГО ПО РАЗДЕЛУ 1				18
ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4	Раздел 2. Инженерно-технические средства физической защиты объектов информатизации	1. Рассмотрение документов ГОСТ в области технической защиты 2. Рассмотрение нормативных документов ФСТЭК в области технической защиты 3. Оформление отчета. Участие в зачет-конференции по учебной практике	Тема 2.1. Инженерно-техническая укрепленность объектов информатизации	9
			Тема 2.2. Применение средств инженерно-технической защиты объектов	9

			информатизации и линий связи информационно-телекоммуникационных систем и сетей (ИТКС)	
ВСЕГО ПО РАЗДЕЛУ 2				18
УП 04.01 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"				108
ПК 4.1 ПК 4.2	Раздел 1. Осуществление установки и базовых настроек операционной системы, периферийных устройств, локальной вычислительной сети	1. Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. 2. Проверка состояния аппаратного обеспечения 3. Подключение устройств ввода вывода 4. Настройка виртуальной машины. Установка операционной системы. 5. Настройка интерфейса. Установка программного обеспечения 6. Подключение и настройка локальной вычислительной сети 7. Создание текстовых документов 8. Создание электронных таблиц 9. Работа с формулами, функциями и списками в электронных таблицах	Тема 1.1 Программное и аппаратное обеспечение ВТ	27
			Тема 1.2 Коммуникационные технологии. Организация работы в глобальной сети Интернет	27
ВСЕГО ПО РАЗДЕЛУ 1				54
	Раздел 2. Выполнение основных действий в прикладных программных продуктах.	1. Создание структуры базы данных в СУБД 2. Управление содержанием баз данных в СУБД	Тема 2.1 Технология хранения, поиска и сортировки	54

		3. Создание презентаций 4. Создание диаграмм и блок-схем 5. Осуществление основных действий по обработке изображений в растровом графическом редакторе 6. Осуществление основных действий по созданию изображений в растровом графическом редакторе 7. Осуществление основных действий по созданию изображений в векторном графическом редакторе 8. Осуществление основных действий по разработке веб-приложений 9. Оформление отчета. Участие в квалификационном экзамене по учебной практике	информации. Базы данных	
ВСЕГО ПО РАЗДЕЛУ 2				54
УП 05.01 Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)"				72
ПК 1.1 ПК 1.2 ПК 2.1 ПК 5.1 ПК 5.2	Раздел 1. Введение в профессию «Оператор беспилотных летательных аппаратов (БПЛА)»	1. Проведение инструктажа по технике безопасности. Получение заданий по тематике 2. Подготовка к эксплуатации элементов беспилотной авиационной системы различных типов: самолетного, мультироторного, смешанного 3. Составление полётных программы с учетом особенностей функционального оборудования полезной	Тема 1. Техническое обслуживание элементов беспилотных воздушных судов и их комплектующих	9
			Тема 2 Нормативно-правовая документация в области беспилотных авиационных систем	9
			Тема 3 Устройство	9

		нагрузки, установленного на беспилотном воздушном судне и характера перевозимого внешнего груза	механических узлов, конструкций и других составляющих БАС	
		4. Ознакомление с процедурами по предупреждению, выявлению и устранению прямых и косвенных причин снижения надежности дистанционно пилотируемых воздушных судов, станции внешнего пилота, систем обеспечения полетов и их функциональных элементов 5. Ознакомление с порядком ведения учёта срока службы, наработки объектов эксплуатации, причин отказов, неисправностей и повреждений беспилотных воздушных судов различных типов: самолетного, мультироторного, смешанного 6. Управлять беспилотным воздушным судном различных типов в пределах его эксплуатационных ограничений	Тема 4 Проведение проверок исправности и работоспособности беспилотных воздушных судов	9
			ВСЕГО ПО РАЗДЕЛУ 1	36
ПК 1.1 ПК 1.2 ПК 2.1 ПК 5.1 ПК 5.2	Раздел 2. Программирование беспилотных авиационных систем	1. Планирование, подготовка и выполнение полетов на дистанционно пилотируемом воздушном судне и	Тема 1. Принципы управления и строения мультикоптеров	18

		автономном воздушном судне различных типов (с различными вариантами проведения взлета и посадки): самолетного, мультироторного, смешанного 2. Техническая эксплуатация дистанционно пилотируемых воздушных судов самолетного типа, станции внешнего пилота, систем обеспечения полетов и их функциональных элементов 3. Обработка данных, полученных при использовании дистанционно пилотируемых воздушных судов 4. Наладка измерительных приборов и контрольно-проверочной аппаратуры 5. Проведение проверок исправности, работоспособности и готовности дистанционно пилотируемых воздушных судов, станции внешнего пилота, систем обеспечения полетов и их функциональных элементов 6. Оформление документации по обслуживанию авиационных систем. Оформления отчета по практике	Тема 2. Программирование взлёта и посадки беспилотного летательного аппарата	18
			ВСЕГО ПО РАЗДЕЛУ 2	36

УП 06.01 Интеграция облачных технологий в цифровую экономику				144
ПК 6.1 ПК 6.4 ПК 6.6	Раздел 1. Квантовая защита данных	1. Аудит безопасности облачной инфраструктуры с учетом квантовых угроз 2. Миграция данных в облако с использованием квантово-устойчивых алгоритмов 3. Интеграция систем квантового распределения ключей (КРК) с облачной инфраструктурой 4. Разработка облачного приложения, защищенного с использованием квантовой криптографии 5. Мониторинг безопасности облачной инфраструктуры с использованием квантовых сенсоров 6. Аудит безопасности алгоритмов, используемых в облачных сервисах, на предмет квантовой устойчивости 7. Разработка решения для безопасного хранения квантовых ключей в облаке 8. Интеграция постквантовых алгоритмов в существующие облачные приложения 9. Разработка системы обнаружения квантовых атак на облачные сервисы 10. Создание политики безопасности для использования квантовых технологий в облаке	Тема 1. Введение в квантовую криптографию	18
			Тема 2. Квантовое распределение ключей (КРК)	181
			Тема 3. Атаки на системы КРК и методы защиты	18
			Тема 4. Практическое применение КРК и перспективы развития	18

		11. Оценка стоимости внедрения квантовой защиты в облачной инфраструктуре 12. Разработка стратегии миграции криптографических систем в облаке на постквантовые алгоритмы		
			ВСЕГО ПО РАЗДЕЛУ 1	72
	Раздел 2. Облачные технологии	1. Понятие облачных вычислений и модели развертывания. 2. Принципы виртуализации и гипервизоры. 3. Архитектуры облачных платформ IaaS/PaaS/SaaS/FaaS. 4. Анализ рисков и уязвимости облачных сервисов 5. Уязвимые места инфраструктуры облака и методы атаки 6. Атаки типа DDoS, phishing, APT. 7. Законодательство РФ и международные нормативы (GDPR, PCI DSS, ISO 27001). 8. Политики безопасности и внутренние регламенты компаний. 9. Сертификация решений облачной безопасности. 10. Организация безопасной среды виртуальных машин 11. Построение комплексной политики защиты облачного приложения 12. Оформление отчёта. Подготовка к защите	Тема 4.2.1. Разработка информационных ресурсов с использованием фреймворков и библиотек	72
			ВСЕГО ПО РАЗДЕЛУ 2	72

2.3. Содержание учебной практики

Наименование разделов профессионального модуля и тем учебной практики	Содержание работ	Объем, ак.ч.
УП 01 ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		108
Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении МДК.01.01 Операционные системы		7
Тема 1.1. Основы теории операционных систем	Содержание	1
	Определение операционной системы. Основные понятия. История развития операционных систем. Виды операционных систем. Классификация операционных систем по разным признакам Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.	
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	Содержание	1
	Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС. Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.	
Тема 1.3. Модульная структура операционных систем, пространство пользователя	Содержание	1
	Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.	
Тема 1.4. Управление памятью	Содержание	1
	Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти	
Тема 1.5. Управление процессами, многопроцессорные системы	Содержание	1
	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	
	Содержание	2

Тема 1.6. Виртуализация и облачные технологии	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования Облачные технологии. Исследования в области виртуализации и облаков	
Раздел 2. Безопасность операционных систем		7
Тема 2.1. Принципы построения защиты информации в операционных системах	Содержание	7
	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Порядок обеспечения безопасности информации при эксплуатации операционных систем. Штатные средства ОС для защиты информации.	
Раздел 3. Особенности работы в современных операционных системах		7
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	Содержание	3
	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX. Операционные системы семейства Mac OS: особенности, преимущества и недостатки. Архитектура Android. Приложения Android Конференция «Современные операционные системы»	
Тема 3.2. Операционная система Windows	Содержание	3
	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	
Тема 3.3. Серверные операционные системы	Содержание	1
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	
Раздел 1. Основы теории баз данных МДК.01.02 Базы данных		4
Тема 1.1. Основные понятия теории баз данных. Модели данных	Содержание	1
	Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования. Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных .Терминология реляционных моделей.	

	Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	
Тема 1.2. Основы реляционной алгебры	Содержание	1
	Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	
Тема 1.3. Базовые понятия и классификация систем управления базами данных	Содержание	1
	Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору)	
Тема 1.4. Целостность данных как ключевое понятие баз данных	Содержание	1
	Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	
Раздел 2. Проектирование баз данных		3
Тема 2.1. Информационные модели реляционных баз данных	Содержание	1
	Типы информационных моделей. Логические модели данных. Физические модели данных.	
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	Содержание	1
	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.	
Тема 2.3. Средства автоматизации проектирования	Содержание	1
	CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования	
Раздел 3. Организация баз данных		4
Тема 3.1. Создание базы данных. Манипулирование данными.	Содержание	2
	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.	
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	Содержание	2
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	
Раздел 4. Управление базой данных с помощью SQL		3
Тема 4.1. Структурированный язык запросов SQL	Содержание	2
	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными Классификация SQL. Встроенный язык SQL	
Тема 4.2. Операторы и функции языка SQL	Содержание	1
	Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции	
Раздел 5. Организация распределённых баз данных		3
Тема 5.1. Архитектуры распределенных баз данных	Содержание	1
	Сетевые и иерархические базы данных. Объектно-ориентированные базы данных. Объектно-реляционная база данных Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных	
Тема 5.2. Серверная часть распределенной базы данных	Содержание	1
	Планирование и развёртывание СУБД для работы с клиентскими приложениями	
Тема 5.3. Клиентская часть распределенной базы данных	Содержание	1
	Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация. Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа.	

Раздел 6. Администрирование и безопасность		4
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	Содержание	1
	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.	
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	Содержание	1
	Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	
Тема 6.3. Механизмы защиты информации в системах управления базами данных	Содержание	1
	Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Средства защиты информации в базах данных	
Тема 6.4. Копирование и перенос данных. Восстановление данных	Содержание	1
	Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных	
Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении МДК.01.03 Сети и системы передачи информации		11
Тема 1.1. Основные понятия и определения	Содержание	3
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	

Тема 1.2. Принципы передачи информации в сетях и системах связи	Содержание	3
	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход	
Тема 1.3. Типовые каналы передачи и их характеристики	Содержание	5
	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	
Раздел 2. Сети передачи данных		10
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	Содержание	5
	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	
Тема 2.2. Беспроводные системы передачи данных	Содержание	3
	Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. WIMAX	
Тема 2.3. Сотовые и спутниковые системы	Содержание	2
	Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.	
Раздел 1. Разработка защищенных автоматизированных (информационных) систем МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		10
Тема 1.1. Основы информационных систем как объекта защиты	Содержание	2
	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. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.	

	Основные особенности современных проектов АИС. Электронный документооборот.	
Тема 1.2. Жизненный цикл автоматизированных систем	Содержание	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. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков. 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.	
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	Содержание	1
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации. Понятие уязвимости угрозы. Классификация уязвимостей.	
Тема 1.4. Основные меры защиты информации в автоматизированных системах	Содержание	1
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	Содержание	1
	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа. Ограничение программной среды. Защита машинных носителей информации Регистрация событий безопасности Обнаружение (предотвращение) вторжений Контроль (анализ) защищенности информации Обеспечение целостности информационной системы и информации	

	Обеспечение доступности информации	
Тема 1.6. Защита информации в распределенных автоматизированных системах	Содержание	2
	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	
Тема 1.7. Особенности разработки информационных систем персональных данных	Содержание	2
	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	
Раздел 2. Эксплуатация защищенных автоматизированных систем.		11
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Содержание	1
	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	
Тема 2.2. Администрирование автоматизированных систем	Содержание	1
	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	Содержание	1
	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	
	Содержание	1

Тема 2.4. Защита от несанкционированного доступа к информации	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД. Классификация автоматизированных систем. Требования по защите информации от НСД для АС Требования защищенности СВТ от НСД к информации Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	
Тема 2.5. СЗИ от НСД	Содержание	1
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам. Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности. Обеспечение целостности информационной системы и информации Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	Содержание	1
	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 Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных	

	(информационных) систем в защищенном исполнении Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	
Тема 2.7. Документация на защищаемую автоматизированную систему	Содержание	1
	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	
Раздел 1. Основы передачи данных в компьютерных сетях МДК.01.05. Эксплуатация компьютерных сетей		7
Тема 1.1. Модели сетевого взаимодействия	Содержание	1
	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI. Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	
Тема 1.2. Физический уровень модели OSI	Содержание	1
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.	
Тема 1.3. Топология компьютерных сетей	Содержание	1
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.	
Тема 1.4. Технологии Ethernet	Содержание	1
	Обзор технологий построения локальных сетей. Технология Ethernet. Физический уровень. Канальный уровень	
Тема 1.5. Технологии коммутации	Содержание	1
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	
Тема 1.6. Сетевой протокол IPv4	Содержание	1
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов. Маршрутизация пакетов IPv4 . Протоколы динамической маршрутизации	
	Содержание	1

Тема 1.7. Скоростные и беспроводные сети	Сеть FDDI. Сеть 100VG-AnyLAN.Сверхвысокоскоростные сети. Беспроводные сети	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet		15
Тема 2.2. Начальная настройка коммутатора	Содержание	2
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора. Начальная конфигурация коммутатора.	
Тема 2.3. Виртуальные локальные сети (VLAN)	Содержание	2
	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP. Функция TrafficSegmentation	
Тема 2.4. Функции повышения надежности и производительности	Содержание	2
	Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP. Агрегирование каналов связи.	
Тема 2.5. Адресация сетевого уровня и маршрутизация	Содержание	2
	Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.	
Тема 2.6. Качество обслуживания (QoS)	Содержание	2
	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	Содержание	2
	Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.	
Тема 2.8. Многоадресная рассылка	Содержание	2
	Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.	
Тема 2.9. Функции управления коммутаторами	Содержание	1
	Управление множеством коммутаторов. Протокол SNMP. RMON (Remote Monitoring). Функция Port Mirroring.	
Раздел 3. Межсетевые экраны		2
Тема 3.1. Межсетевые экраны	Содержание	2
	Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.	
Промежуточная аттестация в форме ...		-
УП 02 ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		72
Раздел 1 Программные и программно-аппаратные средства защиты информации		36

Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание	2
	Предмет и задачи программно-аппаратной защиты информации Основные понятия программно-аппаратной защиты информации Классификация методов и средств программно-аппаратной защиты информации	
Тема 1.2. Стандарты безопасности	Содержание	2
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты) Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.	
Тема 1.3. Защищенная автоматизированная система	Содержание	2
	Автоматизация процесса обработки информации Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Дискреционные модели Мандатные модели	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	Содержание	2
	Источники дестабилизирующего воздействия на объекты защиты Способы воздействия на информацию Причины и условия дестабилизирующего воздействия на информацию	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Содержание	2
	Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД Организация доступа к файлам, контроль доступа и разграничение доступа,	

	иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса	
Тема 1.6 Основы защиты автономных автоматизированных систем	Содержание	2
	Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды Расширение BIOS как средство замыкания программной среды. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	
Тема 1.7 Защита программ от изучения	Содержание	2
	Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение. Задачи защиты от изучения и способы их решения. Защита от отладки. Защита от дизассемблирования Защита от трассировки по прерываниям.	
Тема 1.8 Вредоносное программное обеспечение	Содержание	2
	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch..Бот-неты. Принцип функционирования. Методы обнаружения Классификация антивирусных средств. Сигнатурный и эвристический анализ Защита от вирусов в "ручном режиме". Основные концепции построения систем антивирусной защиты на предприятии	
Тема 1.9 Защита программ и данных от несанкционированного копирования	Содержание	2
	Несанкционированное копирование программ как тип НСД Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении на примере MS Office	
Тема 1.10 Защита информации на машинных носителях	Содержание	2
	Проблема защиты отчуждаемых компонентов ПЭВМ.	

	Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. Создание посекторных образов НЖМД. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов Безвозвратное удаление данных. Принципы и алгоритмы.	
Тема 1.11. Системы обнаружения атак и вторжений	Содержание	2
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ Использование сетевых снифферов в качестве СОВ Аппаратный компонент СОВ Программный компонент СОВ Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
Тема 1.12 Основы построения защищенных сетей	Содержание	5
	Сети, работающие по технологии коммутации пакетов Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	
Тема 1.13 Средства организации VPN	Содержание	5
	Виртуальная частная сеть. Функции, назначение, принцип построения Криптографические и некриптографические средства организации VPN Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
Тема 1.14 Обеспечение безопасности межсетевого взаимодействия	Содержание	2
	Методы защиты информации при работе в сетях общего доступа.	

	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности Основные типы firewall. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций Требования по сертификации межсетевых экранов	
Тема 1.15 Мониторинг систем защиты	Содержание	2
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25 Классификация отслеживаемых событий. Особенности построения систем мониторинга Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
Тема 1.16 Изучение мер защиты информации в информационных системах	Содержание	2
	НЕТ СОДЕРЖАНИЯ	
Раздел 2. Криптографические средства защиты информации		36
Тема 2.1. Введение в криптографию	Содержание	3
	Предмет и задачи криптографии. История криптографии. Основные термины	
Тема 2.1. Методы криптографического защиты информации	Содержание	3
	Классификация основных методов криптографической защиты. Методы симметричного шифрования Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр Методы перестановки. Табличная перестановка, маршрутная перестановка	

	Гаммирование. Гаммирование с конечной и бесконечной гаммами	
Тема 2.3. Криптоанализ	Содержание	3
	Основные методы криптоанализа. Криптографические атаки. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса. Перспективные направления криптоанализа, квантовый криптоанализ.	
Тема 2.4. Поточные шифры и генераторы псевдослучайных чисел	Содержание	3
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
Тема 2.5 Кодирование информации. Компьютеризация шифрования.	Содержание	3
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	
Тема 2.6 Симметричные системы шифрования	Содержание	3
	Общие сведения. Структурная схема симметричных криптографических систем 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 2.7 Асимметричные системы шифрования	Содержание	2
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Элементы теории чисел в криптографии с открытым ключом.	
Тема 2.8 Аутентификация данных. Электронная подпись	Содержание	2
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
Тема 2.9 Алгоритмы обмена ключей и протоколы аутентификации	Содержание	2
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации.	

Тема 2.10 Криптозащита информации в сетях передачи данных	Содержание	2
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
Тема 2.11 Защита информации в электронных платежных системах	Содержание	5
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	
Тема 2.12 Компьютерная стеганография	Содержание	5
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
УП 03 ПМ 03 Защита информации техническими средствами		36
Раздел 1. Техническая защита информации		18
Тема 1.1 Технические каналы утечки информации	Содержание	9
	Предмет и задачи технической защиты информации. Технические каналы утечки информации. Оптический канал утечки информации. Акустический канал утечки информации. Радио-электронный канал утечки информации. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).	
Тема 1.2. Способы и средства защиты информации по техническим каналам утечки информации	Содержание	9
	Способы и средства защиты от утечки информации по акустическому каналу. Способы и средства защиты от утечки информации по оптическому каналу. Способы и средства защиты от утечки информации по эфирному радио-электронному каналу. Способы и средства защиты от утечки информации по проводному радио-электронному каналу Побочные электромагнитные излучения (ПЭМИ). Наводки электромагнитных излучений технических средств. Предотвращение утечки информации с помощью радиопередающих устройств.	

	Организация инженерно-технической защиты информации. Моделирование технических каналов утечки информации.	
Раздел 2. Инженерно-технические средства физической защиты объектов информатизации		18
Тема 2.1. Инженерно-техническая укрепленность объектов информатизации	Содержание	9
	Цели и задачи физической защиты объектов информатизации Общие сведения о комплексах инженерно-технических средств физической защиты. Построение систем внешней инженерно-технической укрепленности объекта. Построение инженерно-технической укрепленности зданий и помещений. Дополнительные требования ИТУ специальных помещений. Построение инфраструктуры объектов ИТУ.	
Тема 2.2. Применение средств инженерно-технической защиты объектов информатизации и линий связи информационно-телекоммуникационных систем и сетей (ИТКС)	Содержание	9
	Система тревожной и охранной сигнализации. Система контроля и управления доступом Система охранного телевидения. Система оповещения и управления эвакуацией Моделирование систем инженерно-технической укрепленности и инженерно-технической защиты информации. Методические рекомендации по организации инженерно-технической укрепленности и инженерно-технической защиты информации объекта защиты.	
Промежуточная аттестация в форме ...		-
УП 04 ПМ 04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"		108
Раздел 1. Осуществление установки и базовых настроек операционной системы, периферийных устройств, локальной вычислительной сети		54
Тема 1.1 Программное и аппаратное обеспечение ВТ	Содержание	27
	Основы теории операционных систем Машинно-зависимые свойства операционных систем	
Тема 1.2 Коммуникационные технологии. Организация работы в глобальной сети Интернет	Содержание	27
	Назначение компьютерной сети. Типы сетей. Топология сети. Технические средства коммуникаций. Организация работы в сети. Сетевые протоколы. Глобальная сеть Интернет	
Раздел 2. Выполнение основных действий в прикладных программных продуктах.		54
Тема 2.1 Технология хранения, поиска и сортировки информации. Базы данных	Содержание	54
	Понятие о базе данных и СУБД. Основные объекты базы данных. Структура базы данных. Режимы работы. Ключевое поле.	

	Сортировка информации, фильтры. Организация поиска и выполнение запроса в базе данных.	
Промежуточная аттестация в форме....		
УП 05.01 ПМ 05 Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)"		72
Раздел 1. Введение в профессию «Оператор беспилотных летательных аппаратов (БПЛА)»		36
Тема 1. Техническое обслуживание элементов беспилотных воздушных судов и их комплектующих	Содержание	9
	Техническое обслуживание элементов беспилотных авиационных систем и их комплектующих	
Тема 2 Нормативно-правовая документация в области беспилотных авиационных систем	Содержание	9
	Законодательные и нормативные документы РФ в области эксплуатации беспилотных авиационных систем	
Тема 3 Устройство механических узлов, конструкций и других составляющих БАС	Содержание	9
	Основные типы конструкции беспилотных авиационных систем самолетного типа Основные типы конструкции беспилотных авиационных систем вертолётного (мультироторного) и смешанного типа	
Тема 4 Проведение проверок исправности и работоспособности беспилотных воздушных судов	Содержание	9
	Обслуживание беспилотных авиационных систем Ручное пилотирование беспилотных авиационных систем Техника безопасности и охрана труда при проведении лётных работ Выполнение полётов на симуляторе Выполнение визуальных полётов	
Раздел 2. Программирование беспилотных авиационных систем		36
Тема 1. Принципы управления и строения мультикоптеров.	Содержание	18
	Беспилотная авиация, дроностроение. Описание квадрокоптеров, их принципы управления и применение. Индивидуальные учебные полеты, полеты в парах, в тройке. Разбор аварийных ситуаций. Индивидуальное пилотирование, полеты в паре, в ройке. Выполнение трюков. Разбор аварийных ситуаций. Программирование взлёта и посадки беспилотного летательного аппарата. Выполнение команд «разворот», «изменение высоты», «изменение позиции». Тестирование программного кода в режимах разворота, изменения высоты и позиции.	

	Программирование группового полёта. Теория: основы группового полета квадрокоптеров. Практика: Изучение типов группового поведения роботов.	
Тема 2. Программирование взлёта и посадки беспилотного летательного аппарата	Содержание	18
	Взаимодействие коптера и вычислительного модуля Системы технического зрения. Аэрофотосъемка, навигация, распознавание жестов. Обзорная лекция Основы навигации в пространстве Основы программирования БЛА. Дополнительные модули. Взаимодействие БЛА и модулей. Обзорная лекция	
Промежуточная аттестация в форме....		
УП 06.01 ПМ 06 Интеграция облачных технологий в цифровую экономику		144
Раздел 1. Квантовая защита данных		72
Тема 1. Введение в квантовую криптографию	Содержание	18
	Актуальность квантовой защиты данных Основы квантовой механики для криптографов	
Тема 2. Квантовое распределение ключей (КРК)	Содержание	18
	Принципы работы КРК Протокол BB84 Протоколы E91 и B92 Архитектура систем КРК Квантовый канал связи Однофотонные источники Детекторы одиночных фотонов Согласование ключей	
Тема 3. Атаки на системы КРК и методы защиты	Содержание	18
	Типы атак на системы КРК Программно-аппаратные средства защиты от атак на КРК Аудит безопасности систем КРК	
Тема 4. Практическое применение КРК и перспективы развития	Содержание	18
	Интеграция КРК с существующими криптографическими системами Использование КРК для защиты критической инфраструктуры Варианты применения КРК в коммерческих и государственных структурах	
Раздел 2. Облачные технологии		72
Тема 4.2.1. Разработка информационных ресурсов с использованием фреймворков и библиотек	Содержание	72
	Понятие безопасности данных Основы резервного копирования и восстановления Особенности работы с файловой системой	

	Виды организации контроля доступа к системам и способы распределения прав Регламентирование и учет доступа к системам. Внутренние и внешние технические способы обеспечения контроля прав пользователей, в том числе распределенные. Основы информационной безопасности веб-ресурсов. Принципы использования электронно-цифровых подписей и работы удостоверяющих центров. Программные средства обеспечения безопасности функционирования веб-приложений. Основные уязвимости веб-приложений Способы защиты веб-приложений от атак. Принципы работы и настройки программного файрволла.	
Промежуточная аттестация в форме ...		-

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение учебной практики

Кабинеты общепрофессиональных дисциплин и профессиональных модулей оснащенные в соответствии с приложением 3 ОПОП-П.

Лаборатории электроники и схемотехники, информационных технологий, программирования и баз данных, защиты информации в автоматизированных системах программными и программно-аппаратными средствами, программных и программно-аппаратных средств обеспечения информационной безопасности оснащенные в соответствии с приложением 3 ОПОП-П.

Мастерские и зоны по видам работ, оснащенные в соответствии с приложением 3 ОПОП-П Эксплуатация беспилотных авиационных систем, Квантовые технологии, Облачные технологии

Оснащенные базы практики (мастерские/зоны по видам работ), оснащенные в соответствии с приложением 3 ОПОП-П.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Александров А.Ю. «Методология и практика применения квантовой криптографии». Москва: Наука, 2021 г.

2. Афанасьев, П.П., Беспилотные летательные аппараты. Основы устройства и функционирования[Текст] /И.С.Голубев, В.Н.Новиков, С.Г.Парафесь, под редакцией Голубева И.С. и Туркина И.К. Издательство МАИ, М, 2023г.

3. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: Белов Е.Б. Организационно-правовое обеспечение информационной безопасности:

учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва: Академия, 2021. - 336 с. (Специальности среднего профессионального образования). - URL: https://academia-library.ru - Текст: электронный

4. Беспилотные авиационные системы (БАС) [Текст] / Утв. генеральным секретарем и опубликовано с его санкции. – Международная организация гражданской авиации, 2023. – 50 с. – ISBN 978-92-9231-780-5 2. Беспилотные летательные аппараты: Методики приближенных расчетов основных параметров и характеристик [Текс]/ В. М. Ильюшко, М. М. Митрахович, А. В. Самков и др; Под общ. ред. В. И. Силкова. – К.: 2024. – 304 с., 56 ил.

5. Булыгин Я.С., Ивлев А.П. «Облачные вычисления и информационная безопасность». Екатеринбург: Уральский федеральный университет, 2021 г.

6. Васильев Л.Н. «Физико-технические аспекты квантовой криптографии». Новосибирск: Издательство НГУ, 2020 г.

7. Волков Д.Е., Калугин В.В. «Защита данных в облачных средах: архитектура, технологии, методики». Москва: Солон-Пресс, 2023 г.

8. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум: учебное

9. Глухов, М. М. Введение в теоретико-числовые методы криптографии / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 3-е изд., стер. — Санкт-Петербург: Лань, 2024. — 396 с. — ISBN 978-5-507-47388-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/367010

10. Давыдов Е.Г., Ильин Г.И. «Безопасность телекоммуникаций на основе квантовых технологий». Москва: Горячая линия-Телеком, 2023 г.

11. Заяц, А. М. Организация беспроводных Ad Hoc и Hot Spot сетей в среде ОС Windows: Иванов М.В., Петров Ю.А. «Основы квантовой криптографии и квантовой информатики». СПб.: БХВ-Петербург, 2021 г.

12. Ильин М. Е. Криптографическая защита информации в объектах информационнойинфраструктуры: учебное издание / Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. - Москва: Академия, 2020. - 288 с. (Специальности среднего профессионального образования). - URL: https://academia-library.ru - Текст: электронный

13. Информатика и информационно-коммуникационные технологии (ИКТ): учеб. пособие / Н.Г. Плотникова. — М.: РИОР: ИНФРА-М, 2023. — 124 с.

14. Информатика: Учебник / Сергеева И.И., Музалевская А.А., Тарасова Н.В., - 2-е изд., перераб. и доп. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2022. - 384 с

15. 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

16. Костров Б. В. Сети и системы передачи информации: учебное издание / Костров Б. В.,

17. Кутузов, О. И. Инфокоммуникационные системы и сети: учебник для спо / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 244 с. — ISBN 978-5-8114-8488-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/176902

18. Лебедев А.А., Казанцев С.Ф. «Методы и средства защиты облачных хранилищ данных». Нижний Новгород: Нижегородский государственный университет, 2021 г.

19. Михайлов А.Л., Фёдоров С.К. «Инженерия безопасности облачных сервисов». Москва: Интернет-Университет Информационных Технологий, 2022 г.

20. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 96 с. — ISBN 978-5-8114-7906-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/167185

21. Никифоров, С. Н. Методы защиты информации. Защищенные сети: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 96 с. — ISBN 978-5-8114-7907-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/167186

22. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 124 с. — ISBN 978-5-8114-8256-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/173803

23. Никифоров, С. Н. Методы защиты информации. Шифрование данных: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 160 с. — ISBN 978-5-507-44449-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/224672

24. Общие виды и характеристики беспилотных летательных аппаратов: справ. пособие[Текст] /А.Г. Гребеников, А.К. Мялица, В.В. Парфенюк и др. 2017. 377 с. – ISBN 978-966-662-157-6

25. Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для спо /. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744

26. Погорелов, В. И. Беспилотные летательные аппараты: нагрузки и нагрев: учебное пособие для среднего профессионального образования / В. И. Погорелов. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 191 с. — (Профессиональное образование). — ISBN 978-5-534-10061-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/516778 22 пособие для спо / Р. Н. Гилязова. — 3-е изд., стер. — Санкт-Петербург: Лань, 2022. — 44 с. — ISBN 978-5-8114-9138-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/187645
пособие для спо / С. П. Хабаров. — Санкт-Петербург: Лань, 2021. — 260 с. — ISBN 978-5-8114-6968-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/153931

27. Прохорова, О. В. Информационная безопасность и защита информации: учебник для спо / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург: Лань, 2023. — 124 с. — ISBN 978-5-507-47174-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/336200

28. Прохорова, О. В. Информационная безопасность и защита информации: учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург: Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082

29. Российские беспилотники // Сайт-портал для консолидации представителей беспилотного сообщества на одном ресурсе, с целью более плотного взаимодействия внутри отрасли и формирования единого информационного поля. - Режим доступа к сайту: https://russiandrone.ru/publications/bespilotnye-letatelnyeapparaty/

30. Ручкин В. Н. - Москва: Академия, 2021. - 256 с. (Специальности среднего профессионального образования). - URL: https://academia-moscow.ru. - Текст: электронный системное администрирование / А. Г. Уймин. — Санкт-Петербург: Лань, 2024. — 116 с. — ISBN 978-5-507-48647-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/362903

31. Соснин, П. И. Архитектурное моделирование автоматизированных систем / П. И. Соснин. — 3-е изд., стер. — Санкт-Петербург: Лань, 2023. — 180 с. — ISBN 978-5-507-46075-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/297017

32. Струмпэ Н.В. Оператор ЭВМ: Практические работы (9 -е изд.) 2022.

Уймин, А. Г. Практикум. Демонстрационный экзамен базового уровня. Сетевое и учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва: Академия, 2021. - 336 с. (Специальности среднего профессионального образования). - URL: https://academia-moscow.ru. - Текст: электронный" *учебное пособие для спо / А. М. Заяц, С. П. Хабаров. — Санкт-Петербург: Лань 2021. — 220 с. — ISBN 978-5-8114-6974-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/153938*

Хабаров, М. Л. Шилкина. — 2-е изд., стер. — Санкт-Петербург: Лань, 2024. — 120 с. — ISBN 978-5-507-47414-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/382067

33. Хабаров, С. П. Основы моделирования беспроводных сетей. Среда OMNeT++: учебное

34. Хабаров, С. П. Основы моделирования технических систем. Среда Simintech / С. П.

35. Царев В.М., Полянская О.Б. «Информационная безопасность облачных вычислений». Москва: Инфра-М, 2022 г.

36. Чиркин А.С. «Современные проблемы квантовой криптографии». Москва: Техносфера, 2022 г.

37. 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]. — URL: https://urait.ru/bcode/543873

3.2.2. Дополнительные источники *(при необходимости)*

6. Википедия — свободная энциклопедия [Электронный ресурс] - режим доступа: http://ru.wikipedia.org (2025).

7. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http://znanium.com/ (2025).

1. Аппаратное обеспечение ЭВМ. Практикум. (для ССУЗов) Струмпэ Н.В., Сидоров В.Д. 2022, 160с.

2. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/
3. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
4. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
5. Журналы Защита информации. Инсайд: Информационно-методический журнал
6. Информационная безопасность регионов: Научно-практический журнал
7. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
8. Информационный портал по безопасности www.SecurityLab.ru.
9. Методические рекомендации Р 102-2024 “Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации” Н.В. Струмпэ. – 5-е изд., стер. – М.: Издательский центр «Академия», 2024. – 112с.
10. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
11. Оператор ЭВМ. Практические работы: учеб. пособие для НПО/
12. Практикум по информатике: учеб. пособие для студ. учреждений сред. проф. образования/ Е.В. Михеева. -14-е изд., стер. – М.: Издательский центр «Академия», 2024. - 384 с.
13. Российский биометрический портал www.biometrics.ru
14. Сайт журнала Информационная безопасность http://www.itsec.ru –
15. Сайт Научной электронной библиотеки www.elibrary.ru
16. Сборник задач и упражнений по информатике: Учебное пособие/В.Д.Колдаев, под ред. Л.Г.Гагариной - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2021. - 256 с Современные операционные системы. Таненбаум Э. 2023, 4-е изд., 1120 с.
17. Справочно-правовая система «Гарант» » www.garant.ru
18. Справочно-правовая система «Консультант Плюс» www.consultant.ru
19. Установка и обслуживание программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования. (СПО) Богомазова Г. Н., 2022, 256с. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
20. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
21. Федеральный портал «Российское образование www.edu.ru
22. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http://znanium.com/ (2025).
23. Электронно-библиотечная система. [Электронный ресурс] – режим доступа: https://znanium.ru/ (2025);
24. Электронно-библиотечная система. [Электронный ресурс] – режим доступа: https://znanium.ru/ (2025).
25. Электронно-библиотечная система. [Электронный ресурс] – режим доступа: https://znanium.ru/ (2025).

3.3. Общие требования к организации учебной практики

Учебная практика проводится в учебно-производственных мастерских, лабораториях и иных структурных подразделениях образовательного учреждения, либо в организациях в специально оборудованных помещениях на

основе договоров между организацией, осуществляющей деятельность по образовательной программе соответствующего профиля (далее – Профильная организация), и образовательным учреждением.

Сроки проведения учебной практики устанавливаются образовательной организацией в соответствии с ОПОП-П по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Учебная практика реализуются в форме практической подготовки и проводятся непрерывно по неделям при условии обеспечения связи между теоретическим обучением и содержанием практики.

3.4 Кадровое обеспечение процесса учебной практики

Учебная практика проводится мастерами производственного обучения и (или) преподавателями дисциплин профессионального цикла.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Индекс УП	Код ПК, ОК	Основные показатели оценки результата	Формы и методы контроля и оценки
УП 01	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. *ПК 1.5* *ПК.1.6* *ПК 1.7* *ПК 1.8* *ПК 1.9* ОК 01 ОК 02 ОК.09	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных)	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		систем в защищенном исполнении *Демонстрировать умения настройки локальные компьютерные сети* *Демонстрировать умения настройки виртуальных компьютерных сетей* *Демонстрировать умения проектировать реляционные базы данных* *Проектировать сети передачи данных* *Пользоваться нормативно-технической документацией в области защиты информации* обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности	

		необходимой технической документации, в том числе на английском языке	
УП 02	ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6. ПК 2.7. ПК 2.8. ОК 01 ОК 02 ОК.09	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		Производить анализ угроз и уязвимостей автоматизированных систем Разработка и внедрение мер защиты информации в автоматизированных системах обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	
УП 03	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4 *ПК 3.5* ОК 01 ОК 02 ОК.09	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		документы в области защиты информации проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; *проводить классификацию автоматизированных систем и выбор средств защиты* обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	

УП 04	ПК 4.1. ПК 4.2. ОК 01 ОК 02 ОК 04 ОК 05 ОК 09	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета Владение актуальными методами работы в профессиональной и смежных сферах оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) Использование современного программного обеспечения в профессиональной деятельности Организовывает работу коллектива и команды Оформляет документы по профессиональной тематике на государственном языке Понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые)	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике
УП 05.01	ПК 1.1 ПК 1.2 ПК 2.1 ПК 5.1 *ПК 5.2* ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 09	Выполнение внешнего осмотра беспилотной авиационной системы и выявление неисправностей. - установка съемного оборудования на борт (снятие съемного оборудования с борта) беспилотного воздушного судна Выполнение текущего ремонта элементов беспилотной авиационной системы.	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		Оценка метеорологической, орнитологической и аэронавигационной обстановки в районе выполнения полетов беспилотным воздушным судном Организовывать и осуществлять предварительную и предполетную подготовку беспилотных воздушных судов смешанного типа *Организовывать и осуществлять эксплуатацию беспилотных воздушных судов вертолетного типа, в том числе в особых условиях и особых случаях в полете* Обоснованность планирования учебной и профессиональной деятельности; соответствие результата выполнения профессиональных задач эталону (стандартам, образцам, алгоритму, условиям, требованиям или ожидаемому результату); степень точности выполнения поставленных задач. Полнота охвата информационных источников; скорость нахождения и достоверность информации; обновляемость и пополняемость знаний, влияющих на результаты учебной и производственной деятельности. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере	

		Осознание своей ответственности за результат коллективной, командной деятельности, готовности к сотрудничеству, использованию опыта коллег; отсутствие негативных отзывы со стороны коллег и руководства. Демонстрация навыков грамотно общения и оформление документации на государственном языке Российской Федерации, принимая во внимание особенности социального и культурного контекста Демонстрация умений понимать тексты на базовые и профессиональные темы; составлять необходимую документацию на государственном и иностранном языках	
УП 06.01	ПК 6.1. ПК 6.2. ПК 6.3. ПК 6.4. ПК 6.5 *ПК 6.6* ОК 01 ОК 02 ОК 04 ОК 05 ОК 09	Сборка и настройка систем квантового распределения ключа Осуществлять подбор соответствующих оптических элементов Выполнять работы по анализу источников ошибок Выполнение работ по реализации связки классической и квантовой систем Применение программных средств обеспечения безопасности информации веб приложений *Обработка запросов заказчика в службе технической поддержки в соответствии с трудовым заданием* Обоснованность планирования учебной и	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		профессиональной деятельности; соответствие результата выполнения профессиональных задач эталону (стандартам, образцам, алгоритму, условиям, требованиям или ожидаемому результату); степень точности выполнения поставленных задач. Полнота охвата информационных источников; скорость нахождения и достоверность информации; обновляемость и пополняемость знаний, влияющих на результаты учебной и производственной деятельности. Осознание своей ответственности за результат коллективной, командной деятельности, готовности к сотрудничеству, использованию опыта коллег; отсутствие негативных отзывы со стороны коллег и руководства. Демонстрация навыков грамотно общения и оформление документации на государственном языке Российской Федерации, принимая во внимание особенности социального и культурного контекста Демонстрация умений понимать тексты на базовые и профессиональные темы; составлять необходимую документацию на государственном и иностранном языках	

ПРИЛОЖЕНИЕ 1.1.1
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПП.01 ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

ПП.02 ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ПП.03 ПМ 03 Защита информации техническими средствами

ПП 04.01 ПМ 04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"

ПП 06.01 ПМ 06 Интеграция облачных технологий в цифровую экономику

2025 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1.1. Цель и место производственной практики в структуре образовательной программы:

Рабочая программа производственной практики (ПП) является частью программы подготовки ППССЗ в соответствии с ФГОС СПО по профессии / специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и реализуется в профессиональном цикле после прохождения междисциплинарных курсов (МДК) в рамках профессиональных модулей в соответствии с учебным планом (п. 5.1. ОПОП-П):

ПП 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	МДК 01.01 Операционные системы МДК 01.02 Базы данных МДК 01.03 Сети и системы передачи данных МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении МДК 01.05 Эксплуатация компьютерных сетей
ПП 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	МДК 02.01 Программные и программно-аппаратные средства защиты информации МДК 02.02 Криптографические средства защиты информации
ПП 03 Защита информации техническими средствами	ПМ 03 Защита информации техническими средствами	МДК 03.01 Техническая защита информации МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации
ПП 04.01 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"	ПМ 04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"	МДК 04.01 Технология создания и обработки цифровой информации
ПП 06.01 Интеграция облачных технологий в цифровую экономику	ПМ 06 Интеграция облачных технологий в цифровую экономику	МДК 06.01 Квантовая защита данных МДК 06.02 Облачная кибербезопасность

Производственная практика направлена на развитие общих (ОК) и профессиональных компетенций (ПК):

Код ОК / ПК	**Наименование ОК / ПК**

ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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	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.
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 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, 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.
ПК 4.1	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.2.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК. 5.1	Организовывать и осуществлять предварительную и предполетную подготовку беспилотных воздушных судов смешанного типа
ПК 5.2	Организовывать и осуществлять эксплуатацию беспилотных воздушных судов смешанного типа, в том числе в особых условиях и особых случаях в полете
ПК 6.1	Сборка и настройка систем квантового распределения ключа
ПК 6.2	Осуществлять подбор соответствующих оптических элементов
ПК 6.3	Выполнять работы по анализу источников ошибок
ПК 6.4	Выполнение работ по реализации связки классической и квантовой систем
ПК 6.5	Применение программных средств обеспечения безопасности информации веб приложений
ПК 6.6	*Обработка запросов заказчика в службе технической поддержки в соответствии с трудовым заданием*

Цель производственной практики: приобретение практического опыта в рамках профессиональных модулей данной ОПОП-П по видам деятельности: «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении», «Защита информации в автоматизированных системах программными и программно-аппаратными средствами», «Защита информации техническими средствами», «Выполнение работ по профессии «Оператор электронно-вычислительных и вычислительных машин»», «Интеграция облачных технологий в цифровую экономику».

1.2. Планируемые результаты освоения учебной практики

Наименование вида деятельности	**Практический опыт / умения**
Эксплуатация автоматизированных	Практический опыт

(информационных) систем в защищенном исполнении	установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем; администрирование автоматизированных систем в защищенном исполнении; эксплуатация компонентов систем защиты информации автоматизированных систем; диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении; Умения осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; обеспечивать работоспособность, обнаруживать и устранять неисправности;
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Практический опыт установка, настройка программных средств защиты информации в автоматизированной систем; обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети; тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации; решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности; работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе; Умения

	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; применять средства гарантированного уничтожения информации; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; 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;
Защита информации техническими средствами	Практический опыт установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации; применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; проведение 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; проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации;

	установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты; Умения применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных 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 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.
Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"	Практический опыт Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах; Установка программно-аппаратных средств защиты информации Настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам; Умения Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации; Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации;
Интеграция облачных технологий в цифровую экономику	Практический опыт Монтаж оборудования систем Первичная настройка и проверка функционирования систем Монтаж программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД; Установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты систем от НД Первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД;

	Текущий, в том числе автоматизированный, контроль функционирования систем с установленными показателями Текущий, в том числе автоматизированный, контроль функционирования с установленными показателями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях; Восстановление процесса функционирования после сбоев и отказов систем, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях; составления базы знаний технической поддержки на основе обрабатываемых прецедентов; *Работы с оборудованием КРК; анализа и оценки угроз в квантовых коммуникациях; разработки и реализации решений по квантовой защите данных* Умения Проводить монтаж (для программных средств - установку) систем, средств и систем защиты систем от НД Проводить первичную настройку и проверку функционирования систем, средств и систем защиты систем от НД; Проводить проверку комплектности систем, средств и систем защиты систем от НД; Проводить текущий контроль показателей и процесса функционирования систем, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях электросвязи, предусмотренный регламентом их эксплуатации; Проводить предусмотренные регламентом работы по восстановлению процесса и параметров функционирования систем, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях; выяснять из беседы с заказчиком и понимать причины возникших аварийных ситуаций с информационным ресурсом; применять установленные правила делового общения при общении с заказчиком; отвечать на запросы заказчика в установленные регламентом сроки; анализировать и решать типовые запросы заказчиков; работать с программным обеспечением по приему, обработке и регистрации запросов заказчика; координировать решение запросов заказчиков со специалистами соответствующих подразделений; объяснять заказчикам пути решения возникшей проблемы; *Настраивать и эксплуатировать оборудование КРК; оценивать безопасность и стойкость систем квантовой криптографии; интегрировать КРК с существующими криптографическими системами;*

В результате прохождения производственной практики по видам деятельности, предусмотренным ФГОС СПО и запросам работодателей, обучающийся должен получить практический опыт (сформировать умения):

1.3. Обоснование часов производственной практики в рамках вариативной части ОПОП-П

Код ПП	Код ПК/дополнительные (ПК*, ПКц)	Практический опыт	Наименование темы практики	Объем часов ПП	Обоснование увеличения объема практики
ПП. 04.01	ПК 4.1. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах ПК 4.2. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	Навыки	Тема 1.1 Программное и аппаратное обеспечение ВТ Тема 1.2 Коммуникационные технологии. Организация работы в глобальной сети Интернет Тема 2.1 Технология хранения, поиска и сортировки информации. Базы данных	108	По запросу работодателя
ПП. 06.01	Нет вариативной части в пм			108	По запросу работодателя
Объем производственной практики в рамках вариативной части ОПОП-П - 216 ак.ч.					

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

2.1. Трудоемкость освоения производственной практики

Код ПП	Объем, ак.ч.	Форма проведения производственной практики (концентрированно/ рассредоточено)	Курс / семестр

ПП. 01	180	концентрированно	3/6
ПП. 02	144	концентрированно	4/7
ПП 03	144	концентрированно	4/7
ПП 04.01	108	концентрированно	2/4
ПП 06.01	108	концентрированно	4/7
Всего ПП	684	Х	Х

2.2. Структура производственной практики

Код ПК	Наименование разделов профессионального модуля	Виды работ	Наименование тем учебной практики	Объем часов
ПП 01. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении				180
ПК 1.1 ПК 1.2. ПК 1.3 ПК 1.4	Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении МДК.01.01 Операционные системы	1. Проведение инструктажа по технике безопасности.	Тема 1.1. Основы теории операционных систем	2
			Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	2
			Тема 1.3. Модульная структура операционных систем, пространство пользователя	2
			Тема 1.4. Управление памятью	2
			Тема 1.5. Управление процессами, многопроцессорные системы	2
			Тема 1.6. Виртуализация и облачные технологии	2

			ВСЕГО ПО РАЗДЕЛУ 1	12
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4	Раздел 2. Безопасность операционных систем	1. Ознакомление с планом проведения учебной практики. Получение заданий по тематике.	Тема 2.1. Принципы построения защиты информации в операционных системах	12
			ВСЕГО ПО РАЗДЕЛУ 2	12
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4	Раздел 3. Особенности работы в современных операционных системах	Установка программного комплекса Secret Net на рабочие компьютеры пользователей. Базовая настройка.	Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	4
			Тема 3.2. Операционная система Windows	4
			Тема 3.3. Серверные операционные системы	4
			ВСЕГО ПО РАЗДЕЛУ 3	12
!!!	Раздел 1. Основы теории баз данных МДК.01.02 Базы данных	Настройка параметров работы программного обеспечения, включая системы управления базами данных (Установка Windows Server 2019 доменных служб AD. Настройка DNS)	Тема 1.1. Основные понятия теории баз данных. Модели данных	2
			Тема 1.2. Основы реляционной алгебры	2
			Тема 1.3. Базовые понятия и классификация систем управления базами данных	2

			Тема 1.4. Целостность данных как ключевое понятие баз данных	
ВСЕГО ПО РАЗДЕЛУ 1				6
	Раздел 2. Проектирование баз данных	Создание учетных записей пользователей в домене. Настройка разграничений доступа.	Тема 2.1. Информационные модели реляционных баз данных	2
			Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	2
			Тема 2.3. Средства автоматизации проектирования	2
ВСЕГО ПО РАЗДЕЛУ 2				6
	Раздел 3. Организация баз данных	Установка сервера базы данных SQL и Postgresql. Установка SNS, создание политик.	Тема 3.1. Создание базы данных. Манипулирование данными.	3
			Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	3
ВСЕГО ПО РАЗДЕЛУ 3				6

	Раздел 4. Управление базой данных с помощью SQL	Изучение, установка и настройка ПАК «Соболь». Инициализация, создание пользователей и назначение ключей. Объединение работы «Соболь» и SNS.	Тема 4.1. Структурированный язык запросов SQL	3
			Тема 4.2. Операторы и функции языка SQL	3
ВСЕГО ПО РАЗДЕЛУ 4				6
	Раздел 5. Организация распределённых баз данных	Работа с «Соболь» с версии 3.0. Сравнительный анализ ПАК «Соболь» версии 3.0 и 4.0. Перепрошивка «Соболь» до версии 4.0.	Тема 5.1. Архитектуры распределенных баз данных	2
			Тема 5.2. Серверная часть распределенной базы данных	2
			Тема 5.3. Клиентская часть распределенной базы данных	2
ВСЕГО ПО РАЗДЕЛУ 5				6
	Раздел 6. Администрирование и безопасность	Настройка контроля целостности операционной систем Windows 10 с применением ПАК «Соболь» версии 4.0	Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	2
			Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	2

			Тема 6.3. Механизмы защиты информации в системах управления базами данных	1
			Тема 6.4. Копирование и перенос данных. Восстановление данных	1
ВСЕГО ПО РАЗДЕЛУ 6				6
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4	Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении МДК.01.03 Сети и системы передачи информации	Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных	Тема 1.1. Основные понятия и определения	6
			Тема 1.2. Принципы передачи информации в сетях и системах связи	6
			Тема 1.3. Типовые каналы передачи и их характеристики	6
ВСЕГО ПО РАЗДЕЛУ 2				18
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4, ПК 1.8	Раздел 2. Сети передачи данных	Настройка средств архивации данных Windows Server 2019	Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	6
			Тема 2.2. Беспроводные системы передачи данных	6
			Тема 2.3. Сотовые и	6

			спутниковые системы	
			ВСЕГО ПО РАЗДЕЛУ 2	18
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4	Раздел 1. Разработка защищенных автоматизированных (информационных) систем МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Проведение аудита защищенности автоматизированной системы	Тема 1.1. Основы информационных систем как объекта защиты.	3
			Тема 1.2. Жизненный цикл автоматизированных систем	3
			Тема 1.3. Угрозы безопасности информации в автоматизированных системах	3
			Тема 1.4. Основные меры защиты информации в автоматизированных системах	3
			Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	3
			Тема 1.6. Защита информации в распределенных автоматизир	1

			ованных системах	
			Тема 1.7. Особенности разработки информационных систем персональных данных	2
ВСЕГО ПО РАЗДЕЛУ 1				18
	Раздел 2. Эксплуатация защищенных автоматизированных систем.	Установка, настройка и эксплуатация Ubuntu Server и Ubuntu Desktop.	Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	3
			Тема 2.2. Администрирование автоматизированных систем	3
			Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	3
			Тема 2.4. Защита от несанкционированного доступа к информации	
			Тема 2.5. СЗИ от НСД	3

			Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	3
			Тема 2.7. Документация на защищаемую автоматизированную систему	3
			ВСЕГО ПО РАЗДЕЛУ 2	18
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4	Раздел 1. Основы передачи данных в компьютерных сетях МДК.01.05. Эксплуатация компьютерных сетей	Настройка разграничения доступа штатными средствами Ubuntu.	Тема 1.1. Модели сетевого взаимодействия	2
			Тема 1.2. Физический уровень модели OSI	2
			Тема 1.3. Топология компьютерных сетей	2
			Тема 1.4. Технологии Ethernet	1
			Тема 1.5. Технологии коммутации	1
			Тема 1.6. Сетевой протокол IPv4	1
			Тема 1.7. Скоростные и беспроводные сети	3
			ВСЕГО ПО РАЗДЕЛУ 1	12
ПК 1.1. ПК 1.2.	Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet	Организация работ с удаленными хранилищами данных и базами данных.	Тема 2.1. Основы коммутации	1

ПК 1.3. ПК 1.4, ПК 1.9			Тема 2.2. Начальная настройка коммутатора	1
			Тема 2.3. Виртуальные локальные сети (VLAN)	1
			Тема 2.4. Функции повышения надежности и производительности	1
			Тема 2.5. Адресация сетевого уровня и маршрутизация	1
			Тема 2.6. Качество обслуживания (QoS)	1
			Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	1
			Тема 2.8. Многоадресная рассылка	1
			Тема 2.9. Функции управления коммутаторами	4
			ВСЕГО ПО РАЗДЕЛУ 2	12
ПК 1.3 ПК 1.5 ПК 1.6	Раздел 3. Межсетевые экраны	Работа в VMware ESXI. Установка виртуальных машин. . Настройка сети, поднятие сетевой инфраструктуры. Vlan. Поднятие l2tp туннеля на Mikrotik RouterOS	Тема 3.1. Межсетевые экраны	12

		Работа с Netstat, Nmap и Wireshark. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев в её работе. Составление многоуровневой схемы топологии созданной сети. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей. Оформление отчета. Участие в зачет-конференции по учебной практике		
ВСЕГО ПО РАЗДЕЛУ 3				12
ПП 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами				144
ПК 2.1 ПК 2.2 ПК 2.3 ПК.2.4 ПК 2.5 ПК.2.6	Раздел 1 Программные и программно-аппаратные средства защиты информации	1. Вводное занятие. Инструктаж по технике безопасности. 2. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах 3. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности 4. Оценка эффективности применяемых программно-аппаратных средств обеспечения	Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	5
			Тема 1.2. Стандарты безопасности	5
			Тема 1.3. Защищенная автоматизированная система	5
			Тема 1.4. Дестабилизирующее воздействие на объекты защиты	5
			Тема 1.5. Принципы программно-аппаратной защиты информации	5

		информационной безопасности 5. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации 6. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	от несанкционированного доступа	
			Тема 1.6 Основы защиты автономных автоматизированных систем	5
			Тема 1.7 Защита программ от изучения	5
			Тема 1.8 Вредоносное программное обеспечение	5
			Тема 1.9 Защита программ и данных от несанкционированного копирования	5
			Тема 1.10 Защита информации на машинных носителях	5
			Тема 1.11. Системы обнаружения атак и вторжений	5
			Тема 1.12 Основы построения защищенных сетей	5
			Тема 1.13 Средства организации VPN	5
			Тема 1.14 Обеспечение безопасности межсетевого	5

			взаимодействия	
			Тема 1.15 Мониторинг систем защиты	1
			Тема 1.16 Изучение мер защиты информации в информационных системах	1
			ВСЕГО ПО РАЗДЕЛУ 1	72
ПК 2.1 ПК 2.2 ПК 2.3 ПК.2.4 ПК 2.5 ПК.2.6	Раздел 2. Криптографические средства защиты информации	1. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. 2. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. 3. Применение математических методов для оценки качества и выбора наилучшего программного средства 4. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи 5. Оформление отчета. Участие в зачет-	Тема 2.1. Введение в криптографию	6
			Тема 2.2. Методы криптографического защиты информации	6
			Тема 2.3. Криптоанализ	6
			Тема 2.4. Поточные шифры и генераторы псевдослучайных чисел	6
			Тема 2.5 Кодирование информации. Компьютеризация шифрования.	6
			Тема 2.6 Симметричные системы шифрования	6
			Тема 2.7 Асимметричные системы шифрования	6
			Тема 2.8	6

		конференции по учебной практике	Аутентификация данных. Электронная подпись	
			Тема 2.9 Алгоритмы обмена ключей и протоколы аутентификации	6
			Тема 2.10 Криптозащита информации в сетях передачи данных	6
			Тема 2.11 Защита информации в электронных платежных системах	6
			Тема 2.12 Компьютерная стеганография	6
ВСЕГО ПО РАЗДЕЛУ 2				72
ПП 03 Защита информации техническими средствами				144
ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4 ПК 3.5	Раздел 1. Техническая защита информации	1. Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике 2. Разработка организационных и технических мероприятий по заданию преподавателя; 3. Разработка основной документации по инженерно-технической защите информации.	Тема 1.1 Технические каналы утечки информации	36
			Тема 1.2. Способы и средства защиты информации по техническим каналам утечки информации	36
ВСЕГО ПО РАЗДЕЛУ 1				72
ПК 3.1 ПК 3.2	Раздел 2. Инженерно-технические средства	1. Рассмотрение документов ГОСТ в	Тема 2.1. Инженерно-	36

ПК 3.3 ПК 3.4	физической защиты объектов информатизации	области технической защиты 2. Рассмотрение нормативных документов ФСТЭК в области технической защиты 3. Оформление отчета. Участие в зачет-конференции по учебной практике	техническая укрепленность объектов информатизации	
			Тема 2.2. Применение средств инженерно-технической защиты объектов информатизации и линий связи информационно-телекоммуникационных систем и сетей (ИТКС)	36
ВСЕГО ПО РАЗДЕЛУ 2				72
ПП 04.01 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"				108
ПК 4.1 ПК 4.2	Раздел 1. Осуществление установки и базовых настроек операционной системы, периферийных устройств, локальной вычислительной сети	1. Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. 2. Проверка состояния аппаратного обеспечения 3. Подключение устройств ввода вывода 4. Настройка виртуальной машины. Установка операционной системы. 5. Настройка интерфейса. Установка программного обеспечения 6. Подключение и настройка локальной вычислительной сети 7. Создание текстовых документов	Тема 1.1 Программное и аппаратное обеспечение ВТ	27
			Тема 1.2 Коммуникационные технологии. Организация работы в глобальной сети Интернет	27

		8. Создание электронных таблиц 9. Работа с формулами, функциями и списками в электронных таблицах		
			ВСЕГО ПО РАЗДЕЛУ 1	54
	Раздел 2. Выполнение основных действий в прикладных программных продуктах.	1. Создание структуры базы данных в СУБД 2. Управление содержанием баз данных в СУБД 3. Создание презентаций 4. Создание диаграмм и блок-схем 5. Осуществление основных действий по обработке изображений в растровом графическом редакторе 6. Осуществление основных действий по созданию изображений в растровом графическом редакторе 7. Осуществление основных действий по созданию изображений в векторном графическом редакторе 8. Осуществление основных действий по разработке веб-приложений 9. Оформление отчета. Участие в квалификационном экзамене по учебной практике	Тема 2.1 Технология хранения, поиска и сортировки информации. Базы данных	54
			ВСЕГО ПО РАЗДЕЛУ 2	54
ПП 06.01 Интеграция облачных технологий в цифровую экономику				108
ПК 6.1 ПК 6.4 ПК 6.6	Раздел 1. Квантовая защита данных	1. Аудит безопасности облачной инфраструктуры с учетом квантовых угроз 2. Миграция данных в облако с использованием	Тема 1. Введение в квантовую криптографию	14
			Тема 2. Квантовое распределен	14

		квантово-устойчивых алгоритмов 3. Интеграция систем квантового распределения ключей (КРК) с облачной инфраструктурой 4. Разработка облачного приложения, защищенного с использованием квантовой криптографии 5. Мониторинг безопасности облачной инфраструктуры с использованием квантовых сенсоров 6. Аудит безопасности алгоритмов, используемых в облачных сервисах, на предмет квантовой устойчивости 7. Разработка решения для безопасного хранения квантовых ключей в облаке 8. Интеграция постквантовых алгоритмов в существующие облачные приложения 9. Разработка системы обнаружения квантовых атак на облачные сервисы 10. Создание политики безопасности для использования квантовых технологий в облаке 11. Оценка стоимости внедрения квантовой защиты в облачной инфраструктуре 12. Разработка стратегии миграции криптографических систем в облаке на постквантовые алгоритмы	ие ключей (КРК)	
			Тема 3. Атаки на системы КРК и методы защиты	14
			Тема 4. Практическое применение КРК и перспективы развития	12

			ВСЕГО ПО РАЗДЕЛУ 1	54
	Раздел 2. Облачные технологии	1. Понятие облачных вычислений и модели развертывания. 2. Принципы виртуализации и гипервизоры. 3. Архитектуры облачных платформ IaaS/PaaS/SaaS/FaaS. 4. Анализ рисков и уязвимости облачных сервисов 5. Уязвимые места инфраструктуры облака и методы атаки 6. Атаки типа DDoS, phishing, APT. 7. Законодательство РФ и международные нормативы (GDPR, PCI DSS, ISO 27001). 8. Политики безопасности и внутренние регламенты компаний. 9. Сертификация решений облачной безопасности. 10. Организация безопасной среды виртуальных машин 11. Построение комплексной политики защиты облачного приложения 12. Оформление отчёта. Подготовка к защите	Тема 4.2.1. Разработка информационных ресурсов с использованием фреймворков и библиотек	54
			ВСЕГО ПО РАЗДЕЛУ 2	54

2.3. Содержание производственной практики

Наименование разделов профессионального модуля и тем учебной практики	Содержание работ	Объем, ак.ч.
ПП 01 ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		180

Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении МДК.01.01 Операционные системы		12
Тема 1.1. Основы теории операционных систем	Содержание	2
	Определение операционной системы. Основные понятия. История развития операционных систем. Виды операционных систем. Классификация операционных систем по разным признакам Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.	
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	Содержание	2
	Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС. Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.	
Тема 1.3. Модульная структура операционных систем, пространство пользователя	Содержание	2
	Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.	
Тема 1.4. Управление памятью	Содержание	2
	Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти	
Тема 1.5. Управление процессами, многопроцессорные системы	Содержание	2
	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	
Тема 1.6. Виртуализация и облачные технологии	Содержание	2
	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования Облачные технологии. Исследования в области виртуализации и облаков	
Раздел 2. Безопасность операционных систем		12

Тема 2.1. Принципы построения защиты информации в операционных системах	Содержание	12
	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Порядок обеспечения безопасности информации при эксплуатации операционных систем. Штатные средства ОС для защиты информации.	
Раздел 3. Особенности работы в современных операционных системах		12
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	Содержание	4
	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX. Операционные системы семейства Mac OS: особенности, преимущества и недостатки. Архитектура Android. Приложения Android Конференция «Современные операционные системы»	
Тема 3.2. Операционная система Windows	Содержание	4
	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	
Тема 3.3. Серверные операционные системы	Содержание	4
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	
Раздел 1. Основы теории баз данных МДК.01.02 Базы данных		6
Тема 1.1. Основные понятия теории баз данных. Модели данных	Содержание	2
	Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования. Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных .Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	
Тема 1.2. Основы реляционной алгебры	Содержание	2
	Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	

Тема 1.3. Базовые понятия и классификация систем управления базами данных	Содержание	1
	Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору)	
Тема 1.4. Целостность данных как ключевое понятие баз данных	Содержание	1
	Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	
Раздел 2. Проектирование баз данных		6
Тема 2.1. Информационные модели реляционных баз данных	Содержание	2
	Типы информационных моделей. Логические модели данных. Физические модели данных.	
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	Содержание	2
	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.	
Тема 2.3. Средства автоматизации проектирования	Содержание	2
	CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования	
Раздел 3. Организация баз данных		6
Тема 3.1. Создание базы данных. Манипулирование данными.	Содержание	3
	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.	
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	Содержание	3
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц.	

	Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	
Раздел 4. Управление базой данных с помощью SQL		6
Тема 4.1. Структурированный язык запросов SQL	Содержание	3
	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными Классификация SQL. Встроенный язык SQL	
Тема 4.2. Операторы и функции языка SQL	Содержание	3
	Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции	
Раздел 5. Организация распределённых баз данных		6
Тема 5.1. Архитектуры распределенных баз данных	Содержание	2
	Сетевые и иерархические базы данных. Объектно-ориентированные базы данных. Объектно-реляционная база данных Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных	
Тема 5.2. Серверная часть распределенной базы данных	Содержание	2
	Планирование и развёртывание СУБД для работы с клиентскими приложениями	
Тема 5.3. Клиентская часть распределенной базы данных	Содержание	2
	Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация. Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа.	
Раздел 6. Администрирование и безопасность		6
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	Содержание	2
	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых	

	процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.	
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	Содержание	2
	Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	
Тема 6.3. Механизмы защиты информации в системах управления базами данных	Содержание	1
	Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Средства защиты информации в базах данных	
Тема 6.4. Копирование и перенос данных. Восстановление данных	Содержание	1
	Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных	
Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении МДК.01.03 Сети и системы передачи информации		18
Тема 1.1. Основные понятия и определения	Содержание	6
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	
Тема 1.2. Принципы передачи информации в сетях и системах связи	Содержание	6
	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход	
Тема 1.3. Типовые каналы передачи и их характеристики	Содержание	6
	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи.	

	Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	
Раздел 2. Сети передачи данных		18
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	Содержание	6
	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	
Тема 2.2. Беспроводные системы передачи данных	Содержание	6
	Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. WIMAX	
Тема 2.3. Сотовые и спутниковые системы	Содержание	6
	Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.	
Раздел 1. Разработка защищенных автоматизированных (информационных) систем МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		18
Тема 1.1. Основы информационных систем как объекта защиты	Содержание	3
	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. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность. Основные особенности современных проектов АИС. Электронный документооборот.	
Тема 1.2. Жизненный цикл автоматизированных систем	Содержание	3
	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.	

	Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков. 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.	
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	Содержание	3
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации. Понятие уязвимости угрозы. Классификация уязвимостей.	
Тема 1.4. Основные меры защиты информации в автоматизированных системах	Содержание	3
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	Содержание	3
	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа. Ограничение программной среды. Защита машинных носителей информации Регистрация событий безопасности Обнаружение (предотвращение) вторжений Контроль (анализ) защищенности информации Обеспечение целостности информационной системы и информации Обеспечение доступности информации	
Тема 1.6. Защита информации в распределенных автоматизированных системах	Содержание	1
	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	
	Содержание	2

Тема 1.7. Особенности разработки информационных систем персональных данных	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	
Раздел 2. Эксплуатация защищенных автоматизированных систем.		18
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Содержание	3
	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	
Тема 2.2. Администрирование автоматизированных систем	Содержание	3
	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	Содержание	3
	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	
Тема 2.4. Защита от несанкционированного доступа к информации	Содержание	3
	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД. Классификация автоматизированных систем. Требования по защите информации от НСД для АС	

	Требования защищенности СВТ от НСД к информации Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	
Тема 2.5. СЗИ от НСД	Содержание	3
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам. Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности. Обеспечение целостности информационной системы и информации Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	Содержание	3
	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 Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	
Тема 2.7. Документация на защищаемую автоматизированную систему	Содержание	3
	Основные эксплуатационные документы защищенных автоматизированных систем.	

	Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	
Раздел 1. Основы передачи данных в компьютерных сетях МДК.01.05. Эксплуатация компьютерных сетей		12
Тема 1.1. Модели сетевого взаимодействия	Содержание	2
	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI. Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	
Тема 1.2. Физический уровень модели OSI	Содержание	2
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.	
Тема 1.3. Топология компьютерных сетей	Содержание	2
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.	
Тема 1.4. Технологии Ethernet	Содержание	1
	Обзор технологий построения локальных сетей. Технология Ethernet. Физический уровень. Канальный уровень	
Тема 1.5. Технологии коммутации	Содержание	1
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	
Тема 1.6. Сетевой протокол IPv4	Содержание	1
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов. Маршрутизация пакетов IPv4 . Протоколы динамической маршрутизации	
Тема 1.7. Скоростные и беспроводные сети	Содержание	3
	Сеть FDDI. Сеть 100VG-AnyLAN.Сверхвысокоскоростные сети. Беспроводные сети	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet		
Тема 2.2. Начальная настройка коммутатора	Содержание	12
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора. Начальная конфигурация коммутатора.	

Тема 2.3. Виртуальные локальные сети (VLAN)	Содержание	1
	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP. Функция TrafficSegmentation	
Тема 2.4. Функции повышения надежности и производительности	Содержание	1
	Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP. Агрегирование каналов связи.	
Тема 2.5. Адресация сетевого уровня и маршрутизация	Содержание	1
	Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.	
Тема 2.6. Качество обслуживания (QoS)	Содержание	1
	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	Содержание	1
	Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.	
Тема 2.8. Многоадресная рассылка	Содержание	1
	Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.	
Тема 2.9. Функции управления коммутаторами	Содержание	4
	Управление множеством коммутаторов. Протокол SNMP. RMON (Remote Monitoring). Функция Port Mirroring.	
Раздел 3. Межсетевые экраны		12
Тема 3.1. Межсетевые экраны	Содержание	12
	Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.	
Промежуточная аттестация в форме ...		-
ПП 02 ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		144
Раздел 1 Программные и программно-аппаратные средства защиты информации		72
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание	5
	Предмет и задачи программно-аппаратной защиты информации Основные понятия программно-аппаратной защиты информации Классификация методов и средств программно-аппаратной защиты информации	
Тема 1.2. Стандарты безопасности	Содержание	5
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите	

	информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты) Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.	
Тема 1.3. Защищенная автоматизированная система	Содержание	5
	Автоматизация процесса обработки информации Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Дискреционные модели Мандатные модели	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	Содержание	5
	Источники дестабилизирующего воздействия на объекты защиты Способы воздействия на информацию Причины и условия дестабилизирующего воздействия на информацию	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Содержание	5
	Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса	
Тема 1.6 Основы защиты автономных автоматизированных систем	Содержание	5
	Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды Расширение BIOS как средство замыкания программной среды. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	

Тема 1.7 Защита программ от изучения	Содержание	5
	Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение. Задачи защиты от изучения и способы их решения. Защита от отладки. Защита от дизассемблирования Защита от трассировки по прерываниям.	
Тема 1.8 Вредоносное программное обеспечение	Содержание	5
	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch..Бот-неты. Принцип функционирования. Методы обнаружения Классификация антивирусных средств. Сигнатурный и эвристический анализ Защита от вирусов в "ручном режиме". Основные концепции построения систем антивирусной защиты на предприятии	
Тема 1.9 Защита программ и данных от несанкционированного копирования	Содержание	5
	Несанкционированное копирование программ как тип НСД Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении на примере MS Office	
Тема 1.10 Защита информации на машинных носителях	Содержание	5
	Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. Создание посекторных образов НЖМД. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов Безвозвратное удаление данных. Принципы и алгоритмы.	
	Содержание	5

Тема 1.11. Системы обнаружения атак и вторжений	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ Использование сетевых снифферов в качестве СОВ Аппаратный компонент СОВ Программный компонент СОВ Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
Тема 1.12 Основы построения защищенных сетей	Содержание	5
	Сети, работающие по технологии коммутации пакетов Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	
Тема 1.13 Средства организации VPN	Содержание	5
	Виртуальная частная сеть. Функции, назначение, принцип построения Криптографические и некриптографические средства организации VPN Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
Тема 1.14 Обеспечение безопасности межсетевого взаимодействия	Содержание	5
	Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности Основные типы firewall. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к	

	каждому хосту исходя из архитектуры и выполняемых функций Требования по сертификации межсетевых экранов	
Тема 1.15 Мониторинг систем защиты	Содержание	1
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25 Классификация отслеживаемых событий. Особенности построения систем мониторинга Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
Тема 1.16 Изучение мер защиты информации в информационных системах	Содержание	1
	НЕТ СОДЕРЖАНИЯ	
Раздел 2. Криптографические средства защиты информации		72
Тема 2.1. Введение в криптографию	Содержание	6
	Предмет и задачи криптографии. История криптографии. Основные термины	
Тема 2.1. Методы криптографического защиты информации	Содержание	6
	Классификация основных методов криптографической защиты. Методы симметричного шифрования Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр Методы перестановки. Табличная перестановка, маршрутная перестановка Гаммирование. Гаммирование с конечной и бесконечной гаммами	
Тема 2.3. Криптоанализ	Содержание	6
	Основные методы криптоанализа. Криптографические атаки. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса. Перспективные направления криптоанализа, квантовый криптоанализ.	
	Содержание	6

Тема 2.4. Поточные шифры и генераторы псевдослучайных чисел	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
Тема 2.5 Кодирование информации. Компьютеризация шифрования.	Содержание	6
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	
Тема 2.6 Симметричные системы шифрования	Содержание	6
	Общие сведения. Структурная схема симметричных криптографических систем 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 2.7 Асимметричные системы шифрования	Содержание	6
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Элементы теории чисел в криптографии с открытым ключом.	
Тема 2.8 Аутентификация данных. Электронная подпись	Содержание	6
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
Тема 2.9 Алгоритмы обмена ключей и протоколы аутентификации	Содержание	6
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации.	
Тема 2.10 Криптозащита информации в сетях передачи данных	Содержание	6
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
Тема 2.11	Содержание	6

Защита информации в электронных платежных системах	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	
Тема 2.12 Компьютерная стеганография	Содержание	6
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
ПП 03 ПМ 03 Защита информации техническими средствами		144
Раздел 1. Техническая защита информации		72
Тема 1.1 Технические каналы утечки информации	Содержание	36
	Предмет и задачи технической защиты информации. Технические каналы утечки информации. Оптический канал утечки информации. Акустический канал утечки информации. Радио-электронный канал утечки информации. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).	
Тема 1.2. Способы и средства защиты информации по техническим каналам утечки информации	Содержание	36
	Способы и средства защиты от утечки информации по акустическому каналу. Способы и средства защиты от утечки информации по оптическому каналу. Способы и средства защиты от утечки информации по эфирному радио-электронному каналу. Способы и средства защиты от утечки информации по проводному радио-электронному каналу Побочные электромагнитные излучения (ПЭМИ). Наводки электромагнитных излучений технических средств. Предотвращение утечки информации с помощью радиопередающих устройств. Организация инженерно-технической защиты информации. Моделирование технических каналов утечки информации.	
Раздел 2. Инженерно-технические средства физической защиты объектов информатизации		72
Тема 2.1. Инженерно-техническая укрепленность объектов информатизации	Содержание	36
	Цели и задачи физической защиты объектов информатизации	

	Общие сведения о комплексах инженерно-технических средств физической защиты. Построение систем внешней инженерно-технической укрепленности объекта. Построение инженерно-технической укрепленности зданий и помещений. Дополнительные требования ИТУ специальных помещений. Построение инфраструктуры объектов ИТУ.	
Тема 2.2. Применение средств инженерно-технической защиты объектов информатизации и линий связи информационно-телекоммуникационных систем и сетей (ИТКС)	Содержание	36
	Система тревожной и охранной сигнализации. Система контроля и управления доступом Система охранного телевидения. Система оповещения и управления эвакуацией Моделирование систем инженерно-технической укрепленности и инженерно-технической защиты информации. Методические рекомендации по организации инженерно-технической укрепленности и инженерно-технической защиты информации объекта защиты.	
Промежуточная аттестация в форме ...		-
ПП 04.01 ПМ 04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"		108
Раздел 1. Осуществление установки и базовых настроек операционной системы, периферийных устройств, локальной вычислительной сети		54
Тема 1.1 Программное и аппаратное обеспечение ВТ	Содержание	27
	Основы теории операционных систем Машинно-зависимые свойства операционных систем	
Тема 1.2 Коммуникационные технологии. Организация работы в глобальной сети Интернет	Содержание	27
	Назначение компьютерной сети. Типы сетей. Топология сети. Технические средства коммуникаций. Организация работы в сети. Сетевые протоколы. Глобальная сеть Интернет	
Раздел 2. Выполнение основных действий в прикладных программных продуктах.		54
Тема 2.1 Технология хранения, поиска и сортировки информации. Базы данных	Содержание	54
	Понятие о базе данных и СУБД. Основные объекты базы данных. Структура базы данных. Режимы работы. Ключевое поле. Сортировка информации, фильтры. Организация поиска и выполнение запроса в базе данных.	
Промежуточная аттестация в форме....		
ПП 06.01 ПМ 06 Интеграция облачных технологий в цифровую экономику		108
Раздел 1. Квантовая защита данных		54
	Содержание	14

Тема 1. Введение в квантовую криптографию	Актуальность квантовой защиты данных Основы квантовой механики для криптографов	
Тема 2. Квантовое распределение ключей (КРК)	Содержание	14
	Принципы работы КРК Протокол BB84 Протоколы E91 и B92 Архитектура систем КРК Квантовый канал связи Однофотонные источники Детекторы одиночных фотонов Согласование ключей	
Тема 3. Атаки на системы КРК и методы защиты	Содержание	14
	Типы атак на системы КРК Программно-аппаратные средства защиты от атак на КРК Аудит безопасности систем КРК	
Тема 4. Практическое применение КРК и перспективы развития	Содержание	14
	Интеграция КРК с существующими криптографическими системами Использование КРК для защиты критической инфраструктуры Варианты применения КРК в коммерческих и государственных структурах	
Раздел 2. Облачные технологии		54
Тема 4.2.1. Разработка информационных ресурсов с использованием фреймворков и библиотек	Содержание	54
	Понятие безопасности данных Основы резервного копирования и восстановления Особенности работы с файловой системой Виды организации контроля доступа к системам и способы распределения прав Регламентирование и учет доступа к системам. Внутренние и внешние технические способы обеспечения контроля прав пользователей, в том числе распределенные. Основы информационной безопасности веб-ресурсов. Принципы использования электронно-цифровых подписей и работы удостоверяющих центров. Программные средства обеспечения безопасности функционирования веб-приложений. Основные уязвимости веб-приложений Способы защиты веб-приложений от атак. Принципы работы и настройки программного файрволла.	
Промежуточная аттестация в форме ...		-

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение производственной практики

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся (далее – Профильные организации).

База прохождения производственной практики должна быть укомплектована оборудованием, техническими средствами обучения в объеме, позволяющем выполнять определенные виды работ, связанные с будущей профессиональной деятельностью обучающихся. База практики должна обеспечивать безопасные условия труда для обучающихся.

При определении мест производственной практики (по профилю специальности) для лиц с ограниченными возможностями здоровья учитываются рекомендации медико-социальной экспертизы, отраженные в индивидуальной программе реабилитации, относительно рекомендованных условий и видов труда.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

(ЭБ АКАДЕМИЯ)

1. Александров А.Ю. «Методология и практика применения квантовой криптографии». Москва: Наука, 2021 г.
2. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности:
3. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва: Академия, 2021. - 336 с. (Специальности среднего профессионального образования). - URL: https://academia-library.ru - Текст: электронный
4. Булыгин Я.С., Ивлев А.П. «Облачные вычисления и информационная безопасность». Екатеринбург: Уральский федеральный университет, 2021 г.
5. Васильев Л.Н. «Физико-технические аспекты квантовой криптографии». Новосибирск: Издательство НГУ, 2020 г.
6. Волков Д.Е., Калугин В.В. «Защита данных в облачных средах: архитектура, технологии, методики». Москва: Солон-Пресс, 2023 г.
7. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум: учебное
8. Глухов, М. М. Введение в теоретико-числовые методы криптографии / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 3-е изд., стер. — Санкт-Петербург: Лань, 2024. — 396 с. — ISBN 978-5-507-47388-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/367010
9. Давыдов Е.Г., Ильин Г.И. «Безопасность телекоммуникаций на основе квантовых технологий». Москва: Горячая линия-Телеком, 2023 г.

10. Заяц, А. М. Организация беспроводных Ad Hoc и Hot Spot сетей в среде ОС Windows:
Иванов М.В., Петров Ю.А. «Основы квантовой криптографии и квантовой информатики». СПб.: БХВ-Петербург, 2021 г.
11. Ильин М. Е. Криптографическая защита информации в объектах

информационнойинфраструктуры: учебное издание / Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. - Москва: Академия, 2020. - 288 с. (Специальности среднего профессионального образования). - URL: https://academia-library.ru - Текст: электронный
12. Информатика и информационно-коммуникационные технологии (ИКТ): учеб. пособие / Н.Г. Плотникова. — М.: РИОР: ИНФРА-М, 2023. — 124 с.
13. Информатика: Учебник / Сергеева И.И., Музалевская А.А., Тарасова Н.В., - 2-е изд., перераб. и доп. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2022. - 384 с
14. 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
15. Костров Б. В. Сети и системы передачи информации: учебное издание / Костров Б. В.,
16. Кутузов, О. И. Инфокоммуникационные системы и сети: учебник для спо / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 244 с. — ISBN 978-5-8114-8488-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/176902
17. Лебедев А.А., Казанцев С.Ф. «Методы и средства защиты облачных хранилищ данных». Нижний Новгород: Нижегородский государственный университет, 2021 г.
18. Михайлов А.Л., Фёдоров С.К. «Инженерия безопасности облачных сервисов». Москва: Интернет-Университет Информационных Технологий, 2022 г.
19. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 96 с. — ISBN 978-5-8114-7906-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/167185
20. Никифоров, С. Н. Методы защиты информации. Защищенные сети: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 96 с. — ISBN 978-5-8114-7907-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/167186
21. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 124 с. — ISBN 978-5-8114-8256-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/173803
22. Никифоров, С. Н. Методы защиты информации. Шифрование данных: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 160 с. — ISBN 978-5-507-44449-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/224672
23. Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для спо /. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744

24. Прохорова, О. В. Информационная безопасность и защита информации: учебник для спо / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург: Лань, 2023. — 124 с. — ISBN 978-5-507-47174-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/336200

25. Прохорова, О. В. Информационная безопасность и защита информации: учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург: Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082

26. Российские беспилотники // Сайт-портал для консолидации представителей беспилотного сообщества на одном ресурсе, с целью более плотного взаимодействия внутри отрасли и формирования единого информационного поля. - Режим доступа к сайту: https://russiandrone.ru/publications/bespilotnye-letatelnyeapparaty/

27. Ручкин В. Н. - Москва: Академия, 2021. - 256 с. (Специальности среднего профессионального образования). - URL: https://academia-moscow.ru. - Текст: электронный системное администрирование / А. Г. Уймин. — Санкт-Петербург: Лань, 2024. — 116 с. — ISBN 978-5-507-48647-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/362903

28. Соснин, П. И. Архитектурное моделирование автоматизированных систем / П. И. Соснин. — 3-е изд., стер. — Санкт-Петербург: Лань, 2023. — 180 с. — ISBN 978-5-507-46075-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/297017

29. Струмпэ Н.В. Оператор ЭВМ: Практические работы (9 -е изд.) 2022. Уймин, А. Г. Практикум. Демонстрационный экзамен базового уровня. Сетевое и учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва: Академия, 2021. - 336 с. (Специальности среднего профессионального образования). - URL: https://academia-moscow.ru. - Текст: электронный" учебное пособие для спо / А. М. Заяц, С. П. Хабаров. — Санкт-Петербург: Лань 2021. — 220 с. — ISBN 978-5-8114-6974-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/153938 Хабаров, М. Л. Шилкина. — 2-е изд., стер. — Санкт-Петербург: Лань, 2024. — 120 с. — ISBN 978-5-507-47414-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/382067

30. Хабаров, С. П. Основы моделирования беспроводных сетей. Среда OMNeT++: учебное

31. Хабаров, С. П. Основы моделирования технических систем. Среда Simintech / С. П.

32. Царев В.М., Полянская О.Б. «Информационная безопасность облачных вычислений». Москва: Инфра-М, 2022 г.

33. Чиркин А.С. «Современные проблемы квантовой криптографии». Москва: Техносфера, 2022 г.

34. 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]. — URL: https://urait.ru/bcode/543873

3.2.2. **Дополнительные источники** (при необходимости)

1.. Википедия — свободная энциклопедия [Электронный ресурс] - режим доступа: http://ru.wikipedia.org (2025).

2. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http://znanium.com/ (2025).

3. Аппаратное обеспечение ЭВМ. Практикум. (для ССУЗов) Струмпэ Н.В., Сидоров В.Д. 2022, 160с.

4. Безопасность информационных технологий. Периодический рецензируемый научный
журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

5. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

6. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных
пользователей;

7. Журналы Защита информации. Инсайд: Информационно-методический журнал

8. Информационная безопасность регионов: Научно-практический журнал

9. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

10. Информационный портал по безопасности www.SecurityLab.ru.

11. Методические рекомендации Р 102-2024 “Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации”
Н.В. Струмпэ. – 5-е изд., стер. – М.: Издательский центр «Академия», 2024. – 112с.

12. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

13. Оператор ЭВМ. Практические работы: учеб. пособие для НПО/

14. Практикум по информатике: учеб. пособие для студ. учреждений сред. проф. образования/ Е.В. Михеева. -14-е изд., стер. – М.: Издательский центр «Академия», 2024. - 384 с.

15. Российский биометрический портал www.biometrics.ru

16. Сайт журнала Информационная безопасность http://www.itsec.ru –

17. Сайт Научной электронной библиотеки www.elibrary.ru

18. Сборник задач и упражнений по информатике: Учебное пособие/В.Д.Колдаев, под ред.
Л.Г.Гагариной - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2021. - 256 с Современные операционные системы. Таненбаум Э. 2023, 4-е изд., 1120 с.

19. Справочно-правовая система «Гарант» » www.garant.ru

20. Справочно-правовая система «Консультант Плюс» www.consultant.ru

21. Установка и обслуживание программного обеспечения персональных компьютеров,
серверов, периферийных устройств и оборудования. (СПО) Богомазова Г. Н., 2022, 256с. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

22. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

23. Федеральный портал «Российское образование www.edu.ru

24. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http://znanium.com/ (2025).

25. Электронно-библиотечная система. [Электронный ресурс] – режим доступа:

https://znanium.ru/ (2025);
26. Электронно-библиотечная система. [Электронный ресурс] – режим доступа: https://znanium.ru/ (2025).
27. Электронно-библиотечная система. [Электронный ресурс] – режим доступа: https://znanium.ru/ (2025).

3.3. Общие требования к организации производственной практики

Производственная практика проводится в профильных организациях на основе договоров, заключаемых между образовательным организацией СПО и профильными организациями.

В период прохождения производственной практики обучающиеся могут зачисляться на вакантные должности, если работа соответствует требованиям программы производственной практики.

Сроки проведения производственной практики устанавливаются образовательной организацией в соответствии с ОПОП-П по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Производственная практика реализуются в форме практической подготовки и проводится непрерывно по неделям при условии обеспечения связи между теоретическим обучением и содержанием практики.

3.4 Кадровое обеспечение процесса производственной практики

Организацию и руководство производственной практикой осуществляют руководители практики от образовательной организации и от профильной организации.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Индекс УП	Код ПК, ОК	Основные показатели оценки результата	Формы и методы контроля и оценки
ПП 01	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. *ПК 1.5* *ПК.1.6* *ПК 1.7* *ПК 1.8* *ПК 1.9* ОК 01 ОК 02 ОК.09	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации 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 *Демонстрировать умения настройки локальные компьютерные сети* *Демонстрировать умения настройки виртуальных компьютерных сетей* *Демонстрировать умения проектировать реляционные базы данных* *Проектировать сети передачи данных* *Пользоваться нормативно-технической документацией в области защиты информации*	

		обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	
ПП 02	ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6. ПК 2.7. ПК 2.8. ОК 01 ОК 02 ОК.09	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными,	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		программно-аппаратными средствами Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак Производить анализ угроз и уязвимостей автоматизированных систем Разработка и внедрение мер защиты информации в автоматизированных системах обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-	

		ресурсы, периодические издания по специальности для решения профессиональных задач эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	
ПП 03	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4 *ПК 3.5* ОК 01 ОК 02 ОК.09	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; *проводить классификацию автоматизированных систем и выбор средств защиты* обоснованность постановки цели, выбора и применения	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	
ПП 04.01	ПК 4.1. ПК 4.2. ОК 01 ОК 02 ОК 04 ОК 05 ОК 09	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета Владение актуальными методами работы в профессиональной и смежных сферах оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		Использование современного программного обеспечения в профессиональной деятельности Организовывает работу коллектива и команды Оформляет документы по профессиональной тематике на государственном языке Понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые)	
ПП 06.01	ПК 6.1. ПК 6.2. ПК 6.3. ПК 6.4. ПК 6.5 *ПК 6.6* ОК 01 ОК 02 ОК 04 ОК 05 ОК 09	Сборка и настройка систем квантового распределения ключа Осуществлять подбор соответствующих оптических элементов Выполнять работы по анализу источников ошибок Выполнение работ по реализации связки классической и квантовой систем Применение программных средств обеспечения безопасности информации веб приложений *Обработка запросов заказчика в службе технической поддержки в соответствии с трудовым заданием* Обоснованность планирования учебной и профессиональной деятельности; соответствие результата выполнения профессиональных задач эталону (стандартам, образцам, алгоритму, условиям, требованиям или ожидаемому результату);	Экспертная оценка демонстрируемых умений, выполняемых действий в процессе учебной и производственной практик Экспертная оценка отчетов по учебной и производственной практике

		степень точности выполнения поставленных задач. Полнота охвата информационных источников; скорость нахождения и достоверность информации; обновляемость и пополняемость знаний, влияющих на результаты учебной и производственной деятельности. Осознание своей ответственности за результат коллективной, командной деятельности, готовности к сотрудничеству, использованию опыта коллег; отсутствие негативных отзывы со стороны коллег и руководства. Демонстрация навыков грамотно общения и оформление документации на государственном языке Российской Федерации, принимая во внимание особенности социального и культурного контекста Демонстрация умений понимать тексты на базовые и профессиональные темы; составлять необходимую документацию на государственном и иностранном языках	