

Приложение 1

к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНЫХ МОДУЛЕЙ

ОГЛАВЛЕНИЕ

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	2
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	36
ПМ.03 Защита информации техническими средствами	64
ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям	90
ПМ.05 Модификация информационных систем	110
ПМ.06 Осуществление интеграции программных модулей	129

Приложение 1.1

к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ)
СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

2025 г.

СОДЕРЖАНИЕ

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ)
СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить основной вид деятельности *Эксплуатация автоматизированных (информационных) систем в защищенном исполнении* и соответствующие ему профессиональные и общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none"> – установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; – администрирования автоматизированных систем в защищенном исполнении; – эксплуатации компонентов систем защиты информации автоматизированных систем; – диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении
уметь	<ul style="list-style-type: none"> – осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении 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
знать	<ul style="list-style-type: none"> – состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; – принципы построения, физические основы работы периферийных устройств; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; – принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 706 час, из них

на освоение МДК – 450 часов, в том числе

на промежуточную аттестацию по МДК – 10 часов,

на практики – 216 часов:

учебная 108 часов;

производственная 108 часоа

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа ¹
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
лабораторных и практических занятий	курсовая работа (проект), часов							
ПК 1.1. ОК 1– ОК 10	Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении	218	214	94	–		–	4
ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 10	Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении	376	392	98	–	108	–	6
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	108					108	–
	Промежуточная аттестация	10	10	–	–	–	–	–
	Экзамен по профессиональному модулю (демонстрационный экзамен)	-	-	–	–	–	–	–
	Всего:	706	616	192	–	108	108	–

Обоснование распределения вариативной части образовательной программы

№ п/п	Код и наименование учебной дисциплины/профессионального модуля	Количество часов	Категория 1. ПОП-П/работодатель 2. ЦОМ/проект	Обоснование
1	ПМ.01 эксплуатация автоматизированных (информационных) систем в защищённом исполнении	115	ПОП-П/работодатель	Для выполнения практикоориентированных заданий, расширения перечня осваиваемых умений, участия в соревнованиях в рамках Регионального чемпионата «Профессионалы»
Итого		115		-

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов
1	2	3
Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении		218
МДК.01.01 Операционные системы		88
Раздел 1. Элементы теории операционных систем. Свойства операционных систем		
Тема 1.1. Основы теории операционных систем	Содержание	4
	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.	
	Содержание	8

Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	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.	
	Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.	
	Тематика практических занятий и лабораторных работ	10
	Виртуальные машины. Создание, модификация, работа	
	Установка ОС	
	Создание и изучение структуры разделов жесткого диска	
	Операции с файлами	
Тема 1.3. Модульная структура операционных систем, пространство пользователя	Содержание	4
	Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.	
	Тематика практических занятий и лабораторных работ	4
	Работа в консольном и графическом режимах	
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	
	Тематика практических занятий и лабораторных работ	2
	Мониторинг за использованием памяти	
Тема 1.5. Управление процессами, многопроцессорные системы	Содержание	4
	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие	
	Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	
	Тематика практических занятий и лабораторных работ	4
	Управление процессами»	

	Наблюдение за использованием ресурсов системы	
Тема 1.6. Виртуализация и облачные технологии	Содержание	4
	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	
	Тематика практических занятий и лабораторных работ	2
	Изучение примеров виртуальных машин (VMware, VBox)	
Раздел 2. Безопасность операционных систем		
Тема 2.1. Принципы построения защиты информации в операционных системах	Содержание	4
	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.	
	Аутентификация, авторизация, аудит.	
	Тематика практических занятий и лабораторных работ	6
	Управление учетными записями пользователей и доступом к ресурсам	
	Аудит событий системы	
	Изучение штатных средств защиты информации в операционных системах	
Раздел 3. Особенности работы в современных операционных системах		
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	Содержание	6
	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	
	Тематика практических занятий и лабораторных работ	4
	Создание дистрибутива Linux. Установка.	
	Работа в ОС Linux.	
	Содержание	2

Тема 3.2. Операционная система Windows	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	
	Тематика практических занятий и лабораторных работ	2
Тема 3.3. Серверные операционные системы	Содержание	2
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	
	Тематика практических занятий и лабораторных работ	4
	Работа с сетевой файловой системой.	
	Работа с серверной ОС, например, AltLinux.	
Примерная тематика самостоятельной работы при изучении МДК.01.01		
1. Создание виртуальной машины. 2. Установка операционной системы. 3. Анализ журнала аудита ОС на рабочем месте. 4. Изучение аналитических обзоров в области построения систем безопасности операционных систем.		2
МДК.01.02 Базы данных		128
Раздел 1. Основы теории баз данных		
Тема 1.1. Основные понятия теории баз данных. Модели данных	Содержание	6
	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	4
	Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	
	Тематика практических занятий и лабораторных работ	4
	Операции над отношениями	
	Содержание	4

Тема 1.2. Базовые понятия и классификация систем управления базами данных	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 1.3. Целостность данных как ключевое понятие баз данных	Содержание Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	4
Раздел 2. Проектирование баз данных		
Тема 2.1. Информационные модели реляционных баз данных	Содержание Типы информационных моделей. Логические модели данных. Физические модели данных.	4
	Тематика практических занятий и лабораторных работ Проектирование инфологической модели данных	2
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	Содержание Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальной формам. Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.	4
	Тематика практических занятий и лабораторных работ Проектирование структуры базы данных	2
Тема 2.3. Средства автоматизации проектирования	Содержание CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	4
	Тематика практических занятий и лабораторных работ Проектирование базы данных с использованием CASE-средств	2
Раздел 3. Организация баз данных		
	Содержание	4

Тема 3.1. Создание базы данных. Манипулирование данными.	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.	
	Тематика практических занятий и лабораторных работ	2
	Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	Содержание	4
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	
	Тематика практических занятий и лабораторных работ	6
	Создание взаимосвязей	
	Сортировка, поиск и фильтрация данных	
	Способы объединения таблиц	
Раздел 4. Управление базой данных с помощью SQL		
Тема 4.1. Структурированный язык запросов SQL	Содержание	4
	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	
	Тематика практических занятий и лабораторных работ	2
	Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL	
Тема 4.2. Операторы и функции языка SQL	Содержание	4
	Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	
	Тематика практических занятий и лабораторных работ	6
	Создание и использование запросов. Группировка и агрегирование данных	
	Коррелированные вложенные запросы	
	Создание в запросах вычисляемых полей. Использование условий	
Раздел 5. Организация распределённых баз данных		

Тема 5.1. Архитектуры распределенных баз данных	Содержание	4
	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.	
	Отличия и преимущества удаленных баз данных от локальных баз данных. Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.	
	Тематика практических занятий и лабораторных работ	2
	Управление доступом к объектам базы данных	
Тема 5.2. Серверная часть распределенной базы данных	Содержание	4
	Планирование и развёртывание СУБД для работы с клиентскими приложениями	
	Тематика практических занятий и лабораторных работ	4
	Установка СУБД. Настройка компонентов СУБД.	
Тема 5.3. Клиентская часть распределенной базы данных	Содержание	4
	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.	
	Оптимизация производительности работы СУБД.	
	Тематика практических занятий и лабораторных работ	6
	Создание форм и отчетов	
	Создание меню. Генерация, запуск.	
	Профилирование запросов клиентских приложений.	
Раздел 6. Администрирование и безопасность		
Тема 6.1. Обеспечение целостности,	Содержание	6
	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения.	

достоверности и непротиворечивости данных.	Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.	
	Тематика практических занятий и лабораторных работ	4
	Разработка хранимых процедур и триггеров	
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	Содержание	4
	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	4
	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	
	Тематика практических занятий и лабораторных работ	4
	Управление правами доступа к базам данных	
Тема 6.4. Копирование и перенос данных. Восстановление данных	Содержание	2
	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	
	Тематика практических занятий и лабораторных работ	4
	Аудит данных с помощью средств СУБД и триггеров	
	Резервное копирование и восстановление баз данных	
Примерная тематика самостоятельной работы при изучении МДК.01.02		2
1. Выполнение индивидуального задания по теме «Проектирование инфологической модели базы данных».		
2. Выполнение индивидуального задания по теме «Нормализация отношений».		
3. Подготовка рефератов на тему «Развитие СУБД» (конкретной СУБД).		

<p>4. Выполнение индивидуального задания по теме «Создание базы данных. Создание таблиц. Организация межтабличных связей»</p> <p>5. Выполнение индивидуального задания по теме «Организация запросов».</p> <p>6. Выполнение индивидуального задания по теме «Создание пользовательского приложения средствами СУБД».</p> <p>7. Разбор синтаксиса хранимых процедур и триггеров.</p> <p>8. Подготовка рефератов по теме «Организация и использование механизмов защиты базы данных».</p>		
<p>Примерные виды самостоятельных работ при изучении раздела 1 модуля</p> <p>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)</p> <p>Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.</p>		
<p>Учебная практика раздела 1 модуля</p> <p>Виды работ</p> <p>1. Установка программного обеспечения в соответствии с технической документацией.</p> <p>2. Настройка параметров работы программного обеспечения, включая системы управления базами данных.</p> <p>3. Настройка компонентов подсистем защиты информации операционных систем.</p> <p>4. Управление учетными записями пользователей.</p> <p>5. Работа в операционных системах с соблюдением действующих требований по защите информации.</p> <p>6. Установка обновления программного обеспечения.</p> <p>7. Контроль целостности подсистем защиты информации операционных систем.</p> <p>8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных</p> <p>9. Использование программных средств для архивирования информации.</p>		36
Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении		282
МДК.01.03 Сети и системы передачи информации		58
Раздел 1. Теория телекоммуникационных сетей		
Тема 1.1. Основные понятия и определения	Содержание	4
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	
	Содержание	6

Тема 1.2. Принципы передачи информации в сетях и системах связи	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	
Тема 1.3. Типовые каналы передачи и их характеристики	Содержание	4
	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезеохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	
	Тематика практических занятий и лабораторных работ	4
	Расчет пропускной способности канала связи	
Раздел 2. Сети передачи данных		
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	Содержание	8
	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.	
	Тематика практических занятий и лабораторных работ	18
	Конфигурирование сетевого интерфейса рабочей станции	
	Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP	
	Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне	
	Диагностика и разрешение проблем сетевого уровня	
	Диагностика и разрешение проблем протоколов транспортного уровня	
Диагностика и разрешение проблем протоколов прикладного уровня		
Тема 2.2. Беспроводные системы передачи данных	Содержание	4
	Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	
	Тематика практических занятий и лабораторных работ	4
	Настройка Wi-Fi маршрутизатора	
Тема 2.3. Сотовые и спутниковые системы	Содержание	4
	Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.	

МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		96
Раздел 1. Разработка защищенных автоматизированных (информационных) систем		
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.	
	Тематика практических занятий и лабораторных работ	2
	Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	
Тема 1.2. Жизненный цикл автоматизированных систем	Содержание	6
	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.	
	Тематика практических занятий и лабораторных работ	2
	Разработка технического задания на проектирование автоматизированной системы	
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	Содержание	2
	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.	
	Тематика практических занятий и лабораторных работ	6

	Категорирование информационных ресурсов	
	Анализ угроз безопасности информации	
	Построение модели угроз	
Тема 1.4. Основные меры защиты информации в автоматизированных системах	Содержание	2
	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	12
	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	
	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	
	Обнаружение (предотвращение) вторжений	
	Контроль (анализ) защищенности информации	
	Обеспечение целостности информационной системы и информации	
	Обеспечение доступности информации	
	Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.	
Защита технических средств.		
Защита информационной системы, ее средств, систем связи и передачи данных		
Резервное копирование и восстановление данных.		
Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.		
	Содержание	2

Тема 1.6. Защита информации в распределенных автоматизированных системах	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 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.	2
	Тематика практических занятий и лабораторных работ	2
	Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	
Раздел 2. Эксплуатация защищенных автоматизированных систем.		
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Содержание 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	4
Тема 2.2. Администрирование автоматизированных систем	Содержание 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.	2
Тема 2.3. Деятельность персонала по эксплуатации	Содержание Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	2

автоматизированных (информационных) систем в защищенном исполнении		
Тема 2.4. Защита от несанкционированного доступа к информации	Содержание	6
	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	8
	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	
	Тематика практических занятий и лабораторных работ	14
	Установка и настройка СЗИ от НСД	
	Защита входа в систему (идентификация и аутентификация пользователей)	
	Разграничение доступа к устройствам	
	Управление доступом	
Использование принтеров для печати конфиденциальных документов. Контроль печати		
Настройка системы для задач аудита		

	Настройка контроля целостности и замкнутой программной среды	
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	
Тема 2.6.	Содержание	8
Эксплуатация средств защиты информации в компьютерных сетях	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	
	Тематика практических занятий и лабораторных работ	2
	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	
Тема 2.7.	Содержание	4
Документация на защищаемую автоматизированную систему	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.	
	Тематика практических занятий и лабораторных работ	4
	Оформление основных эксплуатационных документов на автоматизированную систему.	
Примерная тематика самостоятельной работы при изучении МДК.01.04		4
1. Разработка концепции защиты автоматизированной (информационной) системы		
2. Анализ банка данных угроз безопасности информации		
3. Анализ журнала аудита ОС на рабочем месте		
4. Построение сводной матрицы угроз автоматизированной (информационной) системы		
5. Анализ политик безопасности информационного объекта		
6. Изучение аналитических обзоров в области построения систем безопасности		

7. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации		
МДК.01.05. Эксплуатация компьютерных сетей		108
Раздел 1. Основы передачи данных в компьютерных сетях		
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.	
	Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.	
	Оптоволоконные линии связи	
	Стандарты кабелей. Электрическая проводка.	
	Беспроводная среда передачи.	
	Тематика практических занятий и лабораторных работ	2
	Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	
Сварка оптического волокна		
Тема 1.3. Топология компьютерных сетей	Содержание	2
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.	
	Тематика практических занятий и лабораторных работ	2
	Разработка топологии сети небольшого предприятия	
Построение одноранговой сети		
Тема 1.4. Технологии Ethernet	Содержание	2
	Обзор технологий построения локальных сетей.	
	Технология Ethernet. Физический уровень.	
	Технология Ethernet. Канальный уровень	
	Тематика практических занятий и лабораторных работ	2
Изучение адресации канального уровня. MAC-адреса.		

Тема 1.5. Технологии коммутации	Содержание	2
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI.	
	Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	
	Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети	
	Технология PoweroverEthernet	
	Тематика практических занятий и лабораторных работ	2
	Создание коммутируемой сети	
Тема 1.6. Сетевой протокол IPv4	Содержание	2
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.	
	Маршрутизация пакетов IPv4	
	Протоколы динамической маршрутизации	
	Тематика практических занятий и лабораторных работ	
		Изучение IP-адресации.
Тема 1.7. Скоростные и беспроводные сети	Содержание	2
	Сеть FDDI. Сеть 100VG-AnyLAN	
	Сверхвысокоскоростные сети	
	Беспроводные сети	
	Тематика практических занятий и лабораторных работ	2
	Настройка беспроводного сетевого оборудования	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet		
Тема 2.1. Основы коммутации	Содержание	2
	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов.	
	Управление потоком в полудуплексном и дуплексном режимах.	
	Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов	
	Тематика практических занятий и лабораторных работ	2
	Работа с основными командами коммутатора.	

Тема 2.2. Начальная настройка коммутатора	Содержание	4
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.	
	Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.	
	Тематика практических занятий и лабораторных работ	2
	Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	
	Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	
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.	
	Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation	
	Тематика практических занятий и лабораторных работ	6
	Настройка VLAN на основе стандарта IEEE 802.1Q	
	Настройка протокола GVRP.	
	Настройка сегментации трафика без использования VLAN	
	Настройка функции Q-in-Q (Double VLAN).	
	Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.	
Тема 2.4. Функции повышения надежности и производительности	Содержание	2
	Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.	
	Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.	
	Дополнительные функции защиты от петель. Агрегирование каналов связи.	
	Тематика практических занятий и лабораторных работ	2
	Настройка протоколов связующего дерева STP, RSTP, MSTP.	
	Настройка функции защиты от образования петель LoopBackDetection	
Агрегирование каналов.		

Тема 2.5. Адресация сетевого уровня и маршрутизация	Содержание	2
	Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.	
	Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.	
	Планирование подсетей IPv6. Протокол NDP.	
	Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.	
	Тематика практических занятий и лабораторных работ	6
	Основные конфигурации маршрутизатора.	
	Расширенные конфигурации маршрутизатора.	
	Работа с протоколом CDP.	
	Работа с протоколом TELNET. Работа с протоколом TFTP.	
	Работа с протоколом RIP.	
	Работа с протоколом OSPF.	
	Конфигурирование функции маршрутизатора NAT/PAT.	
	Конфигурирование PPP и CHAP.	
Промежуточная аттестация по МДК.01.05		2
Тема 2.6. Качество обслуживания (QoS)	Содержание	2
	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	
	Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.	
	Тематика практических занятий и лабораторных работ	2
Настройка QoS. Приоритизация трафика. Управление полосой пропускания		
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.	
	Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.	
	Тематика практических занятий и лабораторных работ	2
	Списки управления доступом (AccessControlList)	
Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.		

	Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	
Тема 2.8. Многоадресная рассылка	Содержание	4
	Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.	
	Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping). Функция IGMP FastLeave.	
	Тематика практических занятий и лабораторных работ	2
	Отслеживание трафика многоадресной рассылки.	
	Отслеживание трафика Multicast	
Тема 2.9. Функции управления коммутаторами	Содержание	2
	Управление множеством коммутаторов. Протокол SNMP.	
	RMON (Remote Monitoring). Функция Port Mirroring.	
	Тематика практических занятий и лабораторных работ	2
	Функции анализа сетевого трафика.	
	Настройка протокола управления топологией сети LLDP.	
Раздел 3. Межсетевые экраны		
Тема 3.1. Основные принципы создания надежной и безопасной ИТ- инфраструктуры	Содержание	2
	Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.	
	Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.	
Тема 3.2. Межсетевые экраны	Содержание	2
	Технологии межсетевых экранов. Политика меж сетевого экрана. Межсетевые экраны с возможностями NAT.	
	Топология сети при использовании межсетевых экранов. Планирование и внедрение меж сетевого экрана.	
	Тематика практических занятий и лабораторных работ	4
	Основы администрирования меж сетевого экрана	
	Соединение двух локальных сетей межсетевыми экранами	
	Создание политики без проверки состояния.	
	Создание политик для традиционного (или исходящего) NAT.	

	Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing	
Тема 3.3. Системы обнаружения и предотвращения проникновений	Содержание	2
	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.	
	Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.	
	Тематика практических занятий и лабораторных работ	2
	Обнаружение и предотвращение вторжений.	
Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	Содержание	4
	Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.	
Примерные виды самостоятельных работ при изучении раздела 2 модуля		
Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)		
Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.		
Учебная практика раздела 2 модуля		72
Виды работ		
1. Проведение аудита защищенности автоматизированной системы.		
2. Установка, настройка и эксплуатация сетевых операционных систем.		
3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.		
4. Организация работ с удаленными хранилищами данных и базами данных.		
5. Организация защищенной передачи данных в компьютерных сетях.		
6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.		
7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.		
8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.		

<p>Производственная практика</p> <p>Виды работ:</p> <ol style="list-style-type: none"> 1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения 3. Настройка программного обеспечения с соблюдением требований по защите информации 4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам 5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением 6. Настройка встроенных средств защиты информации программного обеспечения 7. Проверка функционирования встроенных средств защиты информации программного обеспечения 8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения 9. Обслуживание средств защиты информации в компьютерных системах и сетях 10. Обслуживание систем защиты информации в автоматизированных системах 11. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем 12. Проверка работоспособности системы защиты информации автоматизированной системы 13. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации 14. Контроль стабильности характеристик системы защиты информации автоматизированной системы 15. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем 16. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем 	108
<p>Экзамен по профессиональному модулю (демонстрационный экзамен)</p>	-
<p>Всего</p>	706

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы предполагает наличие учебного кабинета, лабораторий информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя;
- посадочные места для обучающихся;
- аудиовизуальный комплекс;
- комплект обучающего материала (комплект презентаций).

Оборудование лаборатории и рабочих мест лаборатории информационных технологий, программирования и баз данных:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- дистрибутив устанавливаемой операционной системы;
- виртуальная машина для работы с операционной системой (гипервизор);
- СУБД;
- CASE-средства для проектирования базы данных;
- инструментальная среда программирования;
- пакет прикладных программ.

Оборудование лаборатории и рабочих мест лаборатории сетей и систем передачи информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- стенды сетей передачи данных;
- структурированная кабельная система;
- эмулятор (эмуляторы) активного сетевого оборудования;
- программное обеспечение сетевого оборудования.

Оборудование лаборатории и рабочих мест лаборатории программных и программно-аппаратных средств защиты информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- антивирусный программный комплекс;
- программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники

1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2022.

2. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2020.
3. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2022.
4. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2022.
5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2022.
6. Сеницын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2020.
7. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2022.
8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2022.

3.2.2. Дополнительные печатные источники:

1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
2. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2012. – 224 с.
3. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб.: Питер, 2006 - 703 с.
4. Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.
5. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2011. – 1024 с.
6. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2011. – 704 с.
7. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2008
8. Кофлер М., Linux. Полное руководство – Питер, 2011. – 800 с.
9. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2008
10. Лапоница О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2007.- 531 с.
11. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.
12. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2005.- 147 с.
13. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2013. – 544 с.
14. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2006. – 240 с.

15. Руссинович М., Соломон Д., Внутреннее устройство Microsoft Windows. Основные подсистемы операционной системы – Питер, 2014. – 672 с.

16. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.

3.2.3. Периодические издания:

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

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

3. Информационная безопасность регионов: Научно-практический журнал

4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности..

URL: <http://cyberrus.com/>

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

3.2.4. Электронные источники:

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

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

3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>

4. Российский биометрический портал www.biometrics.ru

5. Сайт журнала Информационная безопасность <http://www.itsec.ru> –

6. Сайт Научной электронной библиотеки www.elibrary.ru

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

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

9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

10. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>

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

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

<p>ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.</p>	<p>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</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
--	---	--

Приложение 1.2
к ОПОП по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

2025 г.

СОДЕРЖАНИЕ

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ**

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.1.2. Общие компетенции

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none"> – установки, настройки программных средств защиты информации в автоматизированной системе; – обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; – применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; – учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе.
уметь	<ul style="list-style-type: none"> – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – 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
знать	<ul style="list-style-type: none"> – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

	<ul style="list-style-type: none"> – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.
--	--

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 580 час, из них

на освоение МДК – 336 часов, в том числе

на промежуточную аттестацию по МДК – 10 часов,

на практики – 216 часов:

учебная 108 часов;

производственная 108 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа ²
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 2.1 – ПК 2.6 ОК 1-ОК 10	Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации	240	204	60	30	36	–	6
ПК 2.4 ОК 1-ОК 10	Раздел 2 модуля. Применение криптографических средств защиты информации	222	150	74	–	72	–	2
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	108					108	–
	Промежуточная аттестация	10	10	–	–	–	–	–
	Экзамен по профессиональному модулю	-	-	–	–	–	–	–
	Всего:	580	364	134	30	108	108	8

Обоснование распределения вариативной части образовательной программы

№ п/п	Код и наименование учебной дисциплины/профессионального модуля	Количество часов	Категория 1. ПОП-П/работодатель 2. ЦОМ/проект	Обоснование
1	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	81	ПОП-П/работодатель	Для выполнения практикоориентированных заданий, расширения перечня осваиваемых умений, участия в соревнованиях в рамках Регионального чемпионата «Профессионалы»
Итого		81		-

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации		204
МДК.02.01. Программные и программно-аппаратные средства защиты информации		194
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание	4
	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	4
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными	

	<p>средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)</p> <p>Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.</p> <p>Тематика практических занятий и лабораторных работ</p> <p>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.</p> <p>Обзор стандартов. Работа с содержанием стандартов</p>	6
Тема 1.3. Защищенная автоматизированная система	Содержание	4
	Автоматизация процесса обработки информации	
	Понятие автоматизированной системы.	
	Особенности автоматизированных систем в защищенном исполнении.	
	Основные виды АС в защищенном исполнении.	
	Методы создания безопасных систем	
	Методология проектирования гарантированно защищенных КС	
	Дискреционные модели	
	Мандатные модели	
	Тематика практических занятий и лабораторных работ	10
	Учет, обработка, хранение и передача информации в АИС	
	Ограничение доступа на вход в систему.	
	Идентификация и аутентификация пользователей	
	Разграничение доступа.	
	Регистрация событий (аудит).	
Контроль целостности данных		
Уничтожение остаточной информации.		
Управление политикой безопасности. Шаблоны безопасности		
Криптографическая защита. Обзор программ шифрования данных		

	Управление политикой безопасности. Шаблоны безопасности	
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	
	Тематика практических занятий и лабораторных работ	4
	Распределение каналов в соответствии с источниками воздействия на информацию	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Содержание	6
	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	
	Особенности защиты данных от изменения. Шифрование.	
	Тематика практических занятий и лабораторных работ	4
	Организация доступа к файлам	
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	
Раздел 2. Защита автономных автоматизированных систем		
Тема 2.1. Основы защиты автономных автоматизированных систем	Содержание	6
	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)	
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	
Тема 2.2. Защита программ от изучения	Содержание	6
	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 2.3. Вредоносное программное обеспечение	Содержание	6
	Вредоносное программное обеспечение как особый вид разрушающих воздействий	
	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	
	Тематика практических занятий и лабораторных работ	2
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	
Промежуточная аттестация по МДК.02.01		2
Тема 2.4. Защита программ и данных от несанкционированного копирования	Содержание	4
	Несанкционированное копирование программ как тип НСД	
	Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.	
	Привязка ПО к аппаратному окружению и носителям.	
	Защитные механизмы в современном программном обеспечении на примере MS Office	
	Тематика практических занятий и лабораторных работ	2
	Защита информации от несанкционированного копирования с использованием специализированных программных средств	
Защитные механизмы в приложениях (на примере MSWord, MSeXcel, MSPowerPoint)		
Тема 2.5. Защита информации на	Содержание	6
	Проблема защиты отчуждаемых компонентов ПЭВМ.	

машинных носителях	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.	
	Тематика практических занятий и лабораторных работ	8
	Применение средства восстановления остаточной информации на примере Foremost или аналога	
	Применение специализированного программно средства для восстановления удаленных файлов	
	Применение программ для безвозвратного удаления данных	
	Применение программ для шифрования данных на съемных носителях	
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	Содержание	4
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	
	Устройства Touch Memory	
Тема 2.7. Системы обнаружения атак и вторжений	Содержание	6
	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.	
	Тематика практических занятий и лабораторных работ	2
	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	
Раздел 3. Защита информации в локальных сетях		
Тема 3.1. Основы построения защищенных сетей	Содержание	4
	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 3.2. Средства организации VPN	Содержание	4
	Виртуальная частная сеть. Функции, назначение, принцип построения	
	Криптографические и некриптографические средства организации VPN	
	Устройства, образующие VPN. Криptomаршрутизатор и криптофильтр.	
	Крипторouter. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Тематика практических занятий и лабораторных работ	2
Развертывание VPN		
Раздел 4. Защита информации в сетях общего доступа		
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	Содержание	10
	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. Проxy-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	
	Тематика практических занятий и лабораторных работ	4
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	
	Изучение различных способов закрытия "опасных" портов	
Раздел 5. Защита информации в базах данных		
Тема 5.1. Защита информации в базах данных	Содержание	6
	Основные типы угроз. Модель нарушителя	
	Средства идентификации и аутентификации. Управление доступом	
	Средства контроля целостности информации в базах данных	

	Средства аудита и контроля безопасности. Критерии защищенности баз данных	
	Применение криптографических средств защиты информации в базах данных	
	Тематика практических занятий и лабораторных работ	4
	Изучение механизмов защиты СУБД MS Access	
	Изучение штатных средств защиты СУБД MSSQL Server	
Промежуточная аттестация по МДК.02.01		2
Раздел 6. Мониторинг систем защиты		
Тема 6.1. Мониторинг систем защиты	Содержание	6
	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.	
	Тематика практических занятий и лабораторных работ	4
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	
	Проведение аудита ЛВС сетевым сканером	
Тема 6.2. Изучение мер защиты информации в информационных системах	Содержание	2
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	
	Тематика практических занятий и лабораторных работ	4
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	
Тема 6.3. Изучение	Тематика практических занятий и лабораторных работ	12

современных программно-аппаратных комплексов.	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов	
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов	
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	
Курсовая работа		30
Примерная тематика курсовых работ		
<ol style="list-style-type: none"> 1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах 6. Защита сред виртуализации 		
Примерная тематика самостоятельной работы при изучении МДК.02.01		4
<ol style="list-style-type: none"> 1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты 		
Промежуточная аттестация по МДК.02.01		2
Примерные виды самостоятельных работ при изучении раздела 1 модуля		

<p>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)</p> <p>Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.</p> <p>Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.</p>		
<p>Учебная практика по разделу 1 модуля</p> <p>Виды работ:</p> <ul style="list-style-type: none"> – Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах – Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности – Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности – Составление документации по учету, обработке, хранению и передаче конфиденциальной информации – Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации – Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. – Устранение замечаний по результатам проверки – Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. – Применение математических методов для оценки качества и выбора наилучшего программного средства 		36
Раздел 2 модуля. Применение криптографических средств защиты информации		
МДК.02.02. Криптографические средства защиты информации		150
Введение	Содержание	2
	Предмет и задачи криптографии. История криптографии. Основные термины	
Раздел 1. Математические основы защиты информации		
Тема 1.1.	Содержание	24
Математические основы криптографии	Элементы теории множеств. Группы, кольца, поля.	
	Делимость чисел. Признаки делимости. Простые и составные числа.	
	Основная теорема арифметики. Наибольший общий делитель. Взаимно	

	простые числа. Алгоритм Евклида для нахождения НОД.	
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	
	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	
	Китайская теорема об остатках.	
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	Арифметические операции над большими числами.	
	Эллиптические кривые и их приложения в криптографии.	
	Тематика практических занятий и лабораторных работ	8
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	
	Проверка чисел на простоту	
	Решение задач с элементами теории чисел.	
Раздел 2. Классическая криптография		
Тема 2.1. Методы криптографического защиты информации	Содержание	8
	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	
	Тематика практических занятий и лабораторных работ	8
	Применение классических шифров замены	
	Применение классических шифров перестановки	
Применение метода гаммирования		
Тема 2.2. Криптоанализ	Содержание	4
	Основные методы криптоанализа. Криптографические атаки.	
	Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффа	

	Перспективные направления криптоанализа, квантовый криптоанализ.	
	Тематика практических занятий и лабораторных работ	10
	Криптоанализ шифра простой замены методом анализа частотности символов	
	Криптоанализ классических шифров методом полного перебора ключей	
	Криптоанализ шифра Вижинера	
Промежуточная аттестация по МДК.02.02		2
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	Содержание учебного материала	4
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод VBS.	
	Тематика практических занятий и лабораторных работ	4
	Применение методов генерации ПСЧ	
Раздел 3. Современная криптография		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Содержание учебного материала	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	
	Тематика практических занятий и лабораторных работ	8
	Кодирование информации	
	Программная реализация классических шифров	
	Изучение реализации классических шифров замены и перестановки в программе Cryptool или аналоге.	
Тема 3.2. Симметричные системы шифрования	Содержание учебного материала	4
	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	
	Тематика практических занятий и лабораторных работ	4
	Изучение программной реализации современных симметричных шифров	

Тема 3.3. Асимметричные системы шифрования	Содержание учебного материала	4
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	
	Элементы теории чисел в криптографии с открытым ключом.	
	Тематика практических занятий и лабораторных работ	6
	Применение различных асимметричных алгоритмов.	
	Изучение программной реализации асимметричного алгоритма RSA	
Тема 3.4. Аутентификация данных. Электронная подпись	Содержание учебного материала	4
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Тематика практических занятий и лабораторных работ	10
	Применение различных функций хеширования, анализ особенностей хешей	
	Применение криптографических атак на хеш-функции.	
	Изучение программно-аппаратных средств, реализующих основные функции ЭП	
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	Содержание учебного материала	4
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	
	Тематика практических занятий и лабораторных работ	6
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
Тема 3.6. Криптозащита информации в сетях передачи данных	Содержание учебного материала	4
	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.	
	Содержание учебного материала	4

Тема 3.7. Защита информации в электронных платежных системах	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	Тематика практических занятий и лабораторных работ	4
	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	
Тема 3.8. Компьютерная стеганография	Содержание учебного материала	2
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
	Тематика практических занятий и лабораторных работ	2
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	
	Реализация простейших стеганографических алгоритмов	
Примерная тематика самостоятельной работы при изучении МДК.02.02		2
<ol style="list-style-type: none"> 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии 		
Промежуточная аттестация по МДК.02.02		2
Примерные виды самостоятельной работы при изучении раздела 2 модуля		

Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	
Учебная практика раздела 2 модуля Виды работ: – Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	72
Производственная практика по ПМ.02 Виды работ – Анализ принципов построения систем информационной защиты производственных подразделений. – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении – Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	108
Экзамен по профессиональному модулю	
Всего:	580

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы предполагает наличие учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест - 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

Оборудование лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации.

3.2. Информационное обеспечение обучения

3.2.1 Основные печатные источники:

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2022.- 175 с.

2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2022.- 248 с.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2022. – 184 с.

4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2021. – 172 с.

5. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2021. – 336с

6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2021.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

7. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2022. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности
8. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2021
9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2019
10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2022. – 416 с.

3.2.2. Дополнительные печатные источники:

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от

12 июля 2012 г. № 84.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
36. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
38. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
39. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
40. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
41. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
42. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
43. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
44. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
45. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
46. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

47. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

48. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

51. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

3.2.3. Периодические издания:

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

2. Защита информации. Инсайд: Информационно-методический журнал

3. Информационная безопасность регионов: Научно-практический журнал

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

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

3.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

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

3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>

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

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

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

7. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>

8. Российский биометрический портал www.biometrics.ru

9. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>

10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

<p>ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.</p>	<p>Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.</p>	<p>Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>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.</p>	<p>Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.</p>	<p>– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач</p>	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе</p>

<p>ОП 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.</p>	<p>- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач</p>	<p>освоения образовательной программы</p> <p>Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам</p> <p>Экзамен квалификационный</p>
<p>ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.</p>	<p>- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;</p>	
<p>ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.</p>	<p>- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)</p>	
<p>ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.</p>	<p>- грамотность устной и письменной речи, - ясность формулирования и изложения мыслей</p>	
<p>ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.</p>	<p>- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,</p>	
<p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.</p>	<p>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций</p>	
<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания</p>	<p>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;</p>	

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

Приложение 1.3
к ОПОП по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

2025 г.

СОДЕРЖАНИЕ

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ**

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ**

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации техническими средствами* и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации техническими средствами
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none">– установки, монтажа и настройки технических средств защиты информации;– технического обслуживания технических средств защиты информации;– применения основных типов технических средств защиты информации;– выявления технических каналов утечки информации;– участия в мониторинге эффективности технических средств защиты информации;– диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;– проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;– проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;– установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.
уметь	<ul style="list-style-type: none">– применять технические средства для криптографической защиты информации конфиденциального характера;– применять технические средства для уничтожения информации и носителей информации;– применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;– применять инженерно-технические средства физической защиты объектов информатизации
знать	<ul style="list-style-type: none">– порядок технического обслуживания технических средств защиты информации;– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;– порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

	<ul style="list-style-type: none"> – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.
--	---

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 478 час, из них

на освоение МДК – 288 час, в том числе

на промежуточную аттестацию по МДК – 10 часов,

на практики – 180 часов:

учебная 72 часа;

производственная 108 часа

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.03 Защита информации техническими средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа ³
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
лабораторных и практических занятий	курсовая работа (проект), часов							
ПК 3.1- ПК.3.4 ОК 1– ОК10	Раздел 1 модуля. Применение технической защиты информации	180	144	70	–	36	–	2
ПК 3.5 ОК 01– ОК10	Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации	176	140	54	30	36	–	2
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	108					108	–
	Промежуточная аттестация⁴	10	10	–	–	–	–	–
	Экзамен по профессиональному модулю ⁵			–	–	–	–	–

	Всего:	478	294	124	30	72	108	4
--	---------------	------------	------------	-----	----	----	-----	---

5.2.Обоснование распределения вариативной части образовательной программы

№ п/п	Код и наименование учебной дисциплины/профессионального модуля	Количество часов	Категория 1. ПОП-П/работодатель 2. ЦОМ/проект	Обоснование
1	ПМ.03 Защита информации техническими средствами	40	ПОП-П/работодатель	Для выполнения практикоориентированных заданий, расширения перечня осваиваемых умений, участия в соревнованиях в рамках Регионального чемпионата «Профессионалы»
Итого		40		-

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение технической защиты информации		180
МДК.03.01 Техническая защита информации		144
Раздел 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	<p>Содержание</p> <p>Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.</p>	2
Тема 1.2. Общие положения защиты информации техническими средствами	<p>Содержание</p> <p>Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.</p>	4
Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	<p>Содержание</p> <p>Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.</p>	4
Тематика практических занятий и лабораторных работ		4

	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	
Тема 2.2. Технические каналы утечки информации	Содержание	4
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	
	Тематика практических занятий и лабораторных работ	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 2.3. Методы и средства технической разведки	Содержание	4
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Тематика практических занятий и лабораторных работ	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Раздел 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание	6
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика практических занятий и лабораторных работ	4
	Измерение параметров физических полей	
Тема 3.2. Физические процессы при подавлении опасных сигналов	Содержание	2
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Тематика практических занятий и лабораторных работ	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Раздел 4. Системы защиты от утечки информации		

Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание	6
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	
	Тематика практических занятий и лабораторных работ	4
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	Содержание	6
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
	Тематика практических занятий и лабораторных работ	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Промежуточная аттестация по МДК.03.01		2
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	Содержание	6
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Тематика практических занятий и лабораторных работ	4
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание	6
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	
	Тематика практических занятий и лабораторных работ	8
	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	

Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание	6
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Тематика практических занятий и лабораторных работ	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Содержание	6
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Тематика практических занятий и лабораторных работ	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	Содержание	2
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Тематика практических занятий и лабораторных работ	2
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение технических средств защиты информации	Содержание	10
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	
	Тематика практических занятий и лабораторных работ	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
	Содержание	8

Тема 5.2. Эксплуатация технических средств защиты информации	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
	Тематика практических занятий и лабораторных работ	16
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Примерная тематика самостоятельной работы при изучении МДК.03.01		
1.		
Промежуточная аттестация по МДК.03.01		2
Примерные виды самостоятельной работы при изучении раздела 1 модуля		
Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		
Учебная практика Виды работ:		
<ul style="list-style-type: none"> – Измерение параметров физических полей. – Определение каналов утечки ПЭМИН. – Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. – Установка и настройка технических средств защиты информации. – Проведение измерений параметров побочных электромагнитных излучений и наводок. – Проведение аттестации объектов информатизации. 		36
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		208
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		144
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи физической защиты	Содержание	12
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты.	

объектов информатизации	Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	
	Тематика практических занятий и лабораторных работ	2
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание	8
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Тематика практических занятий и лабораторных работ	10
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание	8
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Тематика практических занятий и лабораторных работ	10
	Монтаж датчиков пожарной и охранной сигнализации	
Тема 2.2. Система контроля и управления доступом	Содержание	8
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	
	Тематика практических занятий и лабораторных работ	4
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	

	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	Содержание	6
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
Промежуточная аттестация по МДК.03.02		2
	Тематика практических занятий и лабораторных работ	6
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	Содержание	4
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	
	Тематика практических занятий и лабораторных работ	4
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема 2.5 Система воздействия	Содержание	2
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	
	Тематика практических занятий и лабораторных работ	6
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 3.1 Применение инженерно-технических средств физической защиты	Содержание	4
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	
	Тематика практических занятий и лабораторных работ	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
	Содержание	2

<p>Тема 3.2. Эксплуатация инженерно-технических средств физической защиты</p>	<p>Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.</p>	
	<p>Тематика практических занятий и лабораторных работ</p>	<p>6</p>
	<p>Тематика учебных занятий формируется образовательной организацией самостоятельно</p>	
<p>Курсовой проект (работа)</p>		<p>30</p>
<p>Примерная тематика курсового проекта (работы)</p> <ol style="list-style-type: none"> 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества. 		
<p>Примерная тематика самостоятельной работы при изучении МДК.03.02</p> <ul style="list-style-type: none"> – Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. – Размещение периметровых средств обнаружения на местности. – Самостоятельное изучения порядка допуска субъектов на охраняемые объекты. 		<p>2</p>
<p>Промежуточная аттестация по МДК.03.02</p>		<p>2</p>
<p>Примерные виды самостоятельной работы при изучении раздела 2 модуля</p> <p>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)</p> <p>Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.</p> <p>Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования ...</p>		
<p>Учебная практика по разделу 2 модуля</p> <ol style="list-style-type: none"> 1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 		<p>36</p>

<ol style="list-style-type: none"> 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы шумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации. 	
<p>Производственная практика профессионального модуля</p> <p>Виды работ</p> <ol style="list-style-type: none"> 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съема и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. 	72
<p><i>Экзамен по профессиональному модулю</i></p>	
<p>Всего</p>	478

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

лекционные аудитории с мультимедийным оборудованием; лаборатория «Технических средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест – не менее 30, рабочее место преподавателя, проектор, персональный компьютер, интерактивная доска, комплект презентаций.

Оборудование лаборатории «Технических средств защиты информации» и рабочих мест лаборатории:

- 1) рабочие места студентов, оборудованные персональными компьютерами;
- 2) лабораторные учебные макеты;
- 3) аппаратные средства аутентификации пользователя;
- 4) средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок;
- 5) средства измерения параметров физических полей;
- 6) стенд физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
- 7) рабочее место преподавателя;
- 8) учебно-методическое обеспечение модуля;
- 9) интерактивная доска, комплект презентаций.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2022.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2021.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2020. – 172 с.
4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2021. – 336с
5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2021.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2021
7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2021

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2021. – 416 с.

3.2.2. Дополнительные печатные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
16. Требования о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

27. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

Ростехрегулирование, 2006.

33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

42. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

48. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

49. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

3.2.3 Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» www.garant.ru
6. Федеральный портал «Российское образование» www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
9. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

<p>ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации</p>	<p>Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации</p>	<p>Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.</p>	<p>– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач</p>	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p> <p>Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам</p> <p>Экзамен квалификационный</p>
<p>ОП 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.</p>	<p>- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач</p>	
<p>ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.</p>	<p>- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;</p>	
<p>ОК 04. Работать в коллективе и команде,</p>	<p>- взаимодействие с обучающимися,</p>	

<p>эффективно взаимодействовать с коллегами, руководством, клиентами.</p>	<p>преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)</p>	
<p>ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.</p>	<p>- грамотность устной и письменной речи, - ясность формулирования и изложения мыслей</p>	
<p>ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.</p>	<p>- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,</p>	
<p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.</p>	<p>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций</p>	
<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.</p>	<p>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;</p>	
<p>ОК 09. Использовать информационные технологии в профессиональной деятельности.</p>	<p>- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;</p>	

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	
---	--	--

Приложение 1.4
к ОПОП по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ
ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ**

2025 г.

СОДЕРЖАНИЕ

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ**

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ
ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ**

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих* и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 4	Выполнять работы по профессии «Оператор электронно-вычислительных и вычислительных машин»
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

<p>Иметь практический опыт</p>	<ul style="list-style-type: none"> – выполнения требований техники безопасности при работе с вычислительной техникой; – организации рабочего места оператора электронно-вычислительных и вычислительных машин; – подготовки оборудования компьютерной системы к работе; – инсталляции, настройки и обслуживания программного обеспечения компьютерной системы; – управления файлами; – применения офисного программного обеспечения в соответствии с прикладной задачей; – использования ресурсов локальной вычислительной сети; – использования ресурсов, технологий и сервисов Интернет; – применения средств защиты информации в компьютерной системе.
<p>уметь</p>	<ul style="list-style-type: none"> – выполнять требования техники безопасности при работе с вычислительной техникой; – производить подключение блоков персонального компьютера и периферийных устройств; – производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; – диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; – выполнять инсталляцию системного и прикладного программного обеспечения; – создавать и управлять содержимым документов с помощью текстовых процессоров; – создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; – создавать и управлять содержимым презентаций с помощью редакторов презентаций; – использовать мультимедиа проектор для демонстрации презентаций; – вводить, редактировать и удалять записи в базе данных; – эффективно пользоваться запросами базы данных; – создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; – производить сканирование документов и их распознавание; – производить распечатку, копирование и тиражирование документов на принтере и других устройствах; – управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; – осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; – осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов;

	<ul style="list-style-type: none"> – осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; – осуществлять резервное копирование и восстановление данных.
знать	<ul style="list-style-type: none"> – требования техники безопасности при работе с вычислительной техникой; – основные принципы устройства и работы компьютерных систем и периферийных устройств; – классификацию и назначение компьютерных сетей; – виды носителей информации; – программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета; – основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 402 часа, из них

на практики – 252 часа:

учебная 144 часа;

производственная 108 часов

2. СТРУКТУРА И СОДЕЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа ⁶
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
лабораторных и практических занятий	курсовая работа (проект), часов							
ПК 4.1 – ПК 4.4 ОК1–ОК 10	Раздел 1 модуля. Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»	86	40	68	–	36	–	2
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	72					72	–
	Промежуточная аттестация	10	10	–	–	–	–	–
	Экзамен по профессиональному модулю (демонстрационный экзамен) ⁷			–	–	–	–	–
	Всего:	158	50	68	–	36	72	–

5.2. Обоснование распределения вариативной части образовательной программы

№ п/п	Код и наименование учебной дисциплины/профессионального модуля	Количество часов	Категория 1. ПОП-П/работодатель 2. ЦОМ/проект	Обоснование
18	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям	58	ПОП-П/работодатель	Для выполнения практикоориентированных заданий, расширения перечня осваиваемых умений, участия в соревнованиях в рамках Регионального чемпионата «Профессионалы»
Итого		58		-

2.3. Содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК						
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>						
РАЗДЕЛ 1 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ ПО ПРОФЕССИИ: ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН		158 / 148							
МДК 14.01 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии: Оператор электронно-вычислительных и вычислительных машин		158/ 148							
Тема 1.1. Основы информационных технологий в работе оператора ЭВМ	<p>Содержание. Практические занятия</p> <table border="1" data-bbox="387 794 1576 1193"> <tr> <td data-bbox="387 794 450 943">1</td> <td data-bbox="450 794 1576 943">Профессиональные качества и характеристика профессиональной деятельности оператора ЭВМ Понятие информационных технологий. Цель и инструментарий информационных технологий.</td> </tr> <tr> <td data-bbox="387 943 450 1050">2</td> <td data-bbox="450 943 1576 1050">Развитие информационных технологий. Соотношение между информационными технологиями и информационными системами.</td> </tr> <tr> <td data-bbox="387 1050 450 1193">3</td> <td data-bbox="450 1050 1576 1193">Новая информационная технология. Возможности и ограничения информационных технологий. Данные и информация. Виды информации. Информационный этап развития общества. Единицы измерения информации</td> </tr> </table>	1	Профессиональные качества и характеристика профессиональной деятельности оператора ЭВМ Понятие информационных технологий. Цель и инструментарий информационных технологий.	2	Развитие информационных технологий. Соотношение между информационными технологиями и информационными системами.	3	Новая информационная технология. Возможности и ограничения информационных технологий. Данные и информация. Виды информации. Информационный этап развития общества. Единицы измерения информации	2	ПК 4.1, ОК 01, ОК 02, ОК 03, ОК 05
1	Профессиональные качества и характеристика профессиональной деятельности оператора ЭВМ Понятие информационных технологий. Цель и инструментарий информационных технологий.								
2	Развитие информационных технологий. Соотношение между информационными технологиями и информационными системами.								
3	Новая информационная технология. Возможности и ограничения информационных технологий. Данные и информация. Виды информации. Информационный этап развития общества. Единицы измерения информации								
Тема 1.2. Техническое и программное	<p>Содержание. Практические занятия</p> <p>Практические занятия</p>								

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК
1	2		3	4
обеспечение информационных технологий	1	Операции с файлами и папками в Windows	2	ПК 4.2, ПК 4.3, ПК 4.4ОК 01, ОК 02, ОК 03, ОК 05
	2	Сервисное обслуживание персонального компьютера		
	3	Сервисное обслуживание персонального компьютера		
Тема 1.3 Особенности обработки текстовой информации	Содержание. Практические занятия			
	Практические занятия			ПК 4.1, ПК 4.2, ПК 4.4, ОК.01, ОК.02, ОК.03, ОК.04, ОК.05
	1	Использование шаблонов при подготовке документа. Разметка страницы, нумерация страниц. Проверка правописания	4	
	2	Форматирование абзацев, установка: отступа, интервала, выравнивание		
	3	Редактирование списков: маркированных, нумерованных, многоуровневых		
	4	Редактирование таблиц, представление информации в табличном виде		
	5	Оформление формул с использованием встроенного редактора формул, экспресс-блоков		
	6	Оформление рисунков с использование клипов, фигур, SmartArt		
	7	Оформление документа		
8	Дополнительные возможности программы			

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК	
1	2	3	4	
Тема 1.4. Особенности обработки экономической и статистической информации	Содержание			
	Практические занятия		ПК.1, ПК 4.2, ПК 4.4, ОК.01, ОК.02, ОК.03, ОК.04, ОК.05, ОК.09	
	1	Ввод и редактирование данных. Оформление таблиц	6	
	2	Ввод и редактирование данных. Оформление таблиц		
	3	Расчеты с использованием экономических, статистических и математических функций		
	4	Расчеты с использованием экономических, статистических и математических функций		
	5	Расчеты с использованием экономических, статистических и математических функций		
	6	Связь листов рабочей книги, связь таблиц. Консолидация данных		
	7	Построение диаграмм и графиков		
	8	Построение диаграмм и графиков		
	9	Сводные таблицы, диаграммы и графики		
	10	Сводные таблицы, диаграммы и графики		
11	Инструментарий Поиск решения, Подбор параметра			
	Содержание			

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК	
1	2	3	4	
Тема 1.5 Оформление служебной документации	Практические занятия		ПК 4.1, ПК 4.2, ПК 4.4, ПК 4.3, ОК.01, ОК.02, ОК.03, ОК.04, ОК.05, ОК.09	
	1	Составление бланков документов		4
	2	Оформление организационных документов		
	3	Оформление распорядительных документов		
	4	Оформление справочно-информационных документов		
	5	Оформление писем		
	6	Система электронного документооборота (ЭД)		
	7	Составление документов в системе (ЭД)		
Тема 1.6 Технологии обработки растровой графики	Содержание		ПК 4.1, ПК 4.2, ПК 4.4, ПК 4.3ОК.01, ОК.02, ОК.03, ОК.04, ОК.05, ОК.09	
	Практические занятия			4
	1	Создание графический объектов		
	2	Ретуширование фотографий		
	3	Создание эффектов. Превращение фотоизображения в нарисованное карандашом.		
	4	Редактирование яркости и контраста		

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК
1	2		3	4
	5	Дополнительные возможности программы		
Тема 1.7 Электронные презентации MS PowerPoint	Содержание			
	Практические занятия			ПК 4.1, ПК 4.2, ПК 4.4, ПК 4.3ОК.01, ОК.02, ОК.03, ОК.04, ОК.05, ОК.09
	1	Создание презентации по шаблону	2	
	2	Создание презентаций на определенную тематику с использованием функционала программы		
	5	Настройка презентаций для демонстрации		
6	Разработка интерактивного задания			
Тема 1.8 Технологии обработки аудиоинформации	Содержание			
	Практические занятия			ПК 4.1, ПК 4.2, ПК 4.4, ПК 4.3, ОК.01, ОК.02, ОК.03, ОК.04, ОК.05, ОК.09
	1	Звук. Цифровая запись звука.	2	
	2	Форматы и компрессия звуковых файлов.		
	3	Монтаж аудиоинформации		
4	Монтаж аудиоинформации			

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК	
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	
Тема 1.9 Технологии обработки видеоинформации	Содержание			
	Практические занятия		ПК 4.1, ПК 4.2, ПК 4.4, ПК 4.3ОК.01, ОК.02, ОК.03, ОК.04, ОК.05, ОК.09	
	1	Конвертирование видео-файлов		4
	2	Создание проекта.		
	3	Редактирование проекта.		
4	Обработка видеоинформации.			

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК
1	2	3	4
<p>Учебная практика итоговая по модулю</p> <p>Виды работ</p> <ol style="list-style-type: none"> 1. Создание, форматирование и редактирование документов. Сохранение и открытие документов. Работа со списками и формами документов. Создание и форматирование многоколоночного документа. Создание и импортирование графических объектов в документ. 2. Способы создания таблиц, вычисление в таблицах. Создание сложных документов. Создание математических формул. Форматирование таблиц в ЭТ MS Excel. Создание формул различной сложности. Построение и форматирование диаграмм. Обработка списков: сортировка, фильтрация, консолидация, итоги. Анализ и распределение данных. 3. Создание и настройка слайдов, презентаций, слайд-шоу. Вставка на слайд аудио эффектов, видео, анимации. Использование гиперссылок. 4. Запись и монтаж звука. Улучшение качества звуковой дорожки. Использование эффектов, накладываемых на трек. 5. Выполнение монтажа фильма. Создание различных видеороликов. 6. Установка, настройка, восстановление операционной системы. 7. Подключение периферийных устройств. Установка драйверов периферийных устройств. 8. Технического обслуживания персонального компьютера, принтера, сканера. 9. Санитарные нормы и правила. 10. Определение задач и ресурсов, необходимых для решения данных задач на ЭВМ. 		36	ПК 4.1, ПК 4.2, ПК 4.4, ПК 4.3, ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК
1	2	3	4
<p>Производственная практика итоговая по модулю</p> <p>Виды работ</p> <ol style="list-style-type: none"> 1. Создание, форматирование и редактирование документов. Сохранение и открытие документов. Работа со списками и формами документов. Создание и форматирование многоколоночного документа. Создание и импортирование графических объектов в документ. 2. Создание документа согласно ГОСТ 3. Способы создания таблиц, вычисление в таблицах. Создание сложных документов. Создание математических формул. Форматирование таблиц в ЭТ MS Excel. Создание формул различной сложности. Построение и форматирование диаграмм. Обработка списков: сортировка, фильтрация, консолидация, итоги. Анализ и распределение данных. 4. Создание информационной системы для обработки численной информации 5. Создание и настройка слайдов, презентаций, слайд-шоу. Вставка на слайд аудио эффектов, видео, анимации. 6. Запись и монтаж звука. Выполнение монтажа фильма. 7. Создание интерактивного учебного пособия 8. Технического обслуживания персонального компьютера, принтера, сканера 		72	ПК 4.1, ПК 4.2, ПК 4.4, ПК 4.3ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09
Промежуточная аттестация		10	
Всего		158	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация примерной программы модуля предполагает наличие лаборатории информационных технологий.

Оборудование лаборатории информационных технологий:

Компьютеры, объединенные в локальную вычислительную сеть, проектор, экран, акустическая система.

Программное обеспечение: (операционные системы, пакет прикладных программ, графические редакторы, справочная правовая система, браузер, антивирусная программа)

Учебно-наглядные пособия: схемы, таблицы, учебные презентации

Раздаточный дидактический материал: учебные карточки с заданиями, дидактический материал для выполнения практических работ.

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные источники:

1. Коньков, К. А. Устройство и функционирование ОС Windows. Практикум к курсу Операционные системы. /Учебное пособие // К.А. Коньков. М.: Бином, Лаборатория знаний Интуит, 2019.
2. Струмпэ Н.В. Оператор ЭВМ. Практические работы: учеб. пособие для нач. проф. образования / – 6-е изд., стер. – М.: Издательский центр «Академия», 2019.
3. Киселев С.В. Оператор ЭВМ: учеб. пособие для студ. учреждений сред. проф. образования /. – 7-е изд., испр. – М.: Издательский центр «Академия», 2019.

3.2.2. Дополнительные печатные источники:

1. Жмакин А. П. Архитектура ЭВМ : учеб. пособие для вузов / А. П. Жмакин. - 2-е изд., перераб. и доп. - СПб. : БХВ-Перербург, 2010. - 352 с. : ил. - (Учебная литература для вузов)
2. Сафонов, В.О. Основы современных операционных систем: учебное пособие. М.: Бином. Лаборатория знаний, 2014. – 583 с.
3. Уваров, С. 500 лучших программ для вашего компьютера (2 CD) / С. Уваров. СПб.: Питер, 2009. – 320 с.

3.2.3. Электронные источники:

1. Информационный портал по безопасности www.SecurityLab.ru.
2. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
3. Сайт Научной электронной библиотеки www.elibrary.ru
4. Справочно-правовая система «Гарант» » www.garant.ru
5. Справочно-правовая система «Консультант Плюс» www.consultant.ru
6. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
7. Федеральный портал «Российское образование www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	Демонстрировать умения практические навыки в подготовке оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 4.2 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	Проявление умения и практического опыта в работе с текстовыми документами, таблицами и презентациями, а также базами данных	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ,

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.		оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе	Применение средств защиты информации в компьютерной системе	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОП 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;	

	- обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

Рабочая программа профессионального модуля

«ПМ. 05 МОДИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ»

2025 г.

СОДЕРЖАНИЕ ПРОГРАММЫ

1. Общая характеристика рабочей программы профессионального модуля
2. Структура и содержание профессионального модуля 8
3. Условия реализации профессионального модуля
4. Контроль и оценка результатов освоения профессионального модуля

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ. 13 Модификация информационных систем»

1.1. Цель и место профессионального модуля в структуре образовательной программы
Цель модуля: освоение вида деятельности «Модификация информационных систем» и соответствующие ему общие и профессиональные компетенции.

Профессиональный модуль включён в вариативную часть образовательной программы

1.2. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОПОП-П).

В результате освоения профессионального модуля обучающийся должен:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК.01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части; определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы;	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте;	-
ОК.02	определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска;	Номенклатуру информационных источников, применяемых в профессиональной деятельности; формат оформления результатов поиска информации	-
ОК.04	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	психологические основы деятельности коллектива; психологические особенности личности	-

ОК.09	<p>понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснять свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы</p>	<p>лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности.</p>	-
ПК 5.1.	<p>Осуществлять сопровождение и настройку информационной системы согласно технической документации. Оформлять программную и техническую документацию с использованием стандартов оформления программной документации.</p>	<p>Осуществлять сопровождение и настройку информационной системы согласно технической документации. Оформлять программную и техническую документацию с использованием стандартов оформления программной документации.</p>	<p>Анализировать требования к новой функциональности. Определять, какие модули необходимо модифицировать и в каком направлении. Разработать новые модули или изменять существующие в соответствии с требованиями. Документировать произведенные изменения, содержащие описание новых функций, изменений в коде, описание тестовых случаев и результаты тестирования.</p>
ПК 5.2.	<p>Проводить анализ предметной области. Применять документацию систем качества. Применять основные правила и документы системы сертификации Российской Федерации.</p>	<p>Характеристики и атрибуты качества. Национальная и международная система стандартизации и сертификации и система обеспечения качества продукции, методы контроля качества, в т.ч.</p>	<p>Проводить анализ данных для оценки качества и эффективности информационной системы. Работать с программным обеспечением для</p>

		<p>виды документов по эксплуатации информационной системы;</p> <p>основные языки программирования, используемые для модификации информационных систем.</p>	<p>анализа производительности и оптимизации работы информационной системы.</p>
ПК 5.3.	<p>Составлять проектную документацию на модификацию информационной системы.</p> <p>Применять полученные знания для решения задач по разработке и модернизации информационной системы</p>	<p>Требования к проектной документации.</p> <p>Регламенты по обновлению и техническому сопровождению обслуживаемой информационной системы.</p> <p>Типы тестирования.</p> <p>Особенности программных средств, используемых в разработке информационных систем.</p>	<p>Проводить анализ данных и составлять отчетную документацию по результатам анализа.</p> <p>Разрабатывать проектную документацию на модификацию информационной системы.</p>
ПК 5.4.	<p>применять информационные сервисы в профессиональной деятельности</p>	<p>основные технологические составляющие цифровой экономики;</p> <p>инструменты коммуникации в цифровой экономике;</p> <p>методы и средства защиты информации</p>	<p>Выявлять основные тенденции в развитии современной мировой экономики.</p> <p>Анализировать последствия управленческих решений в сфере бизнеса в условиях цифровизации экономики.</p> <p>Осуществлять поиск, анализ и управление информацией в цифровой среде.</p>

2. Структура и содержание профессионального модуля

2.1. Трудоемкость освоения модуля

Наименование составных частей модуля	Объем в часах	В т.ч. в форме практической подготовки
Учебные занятия	148	68
Самостоятельная работа	10	-
Практика, в т.ч.:	108	108
учебная	36	36
производственная	72	72
Промежуточная аттестация, в том числе:	20	-
Всего	286	176

2.2. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т. ч. в форме практической подготовки	Обучение по МДК	Учебные занятия	Курсовых работ (проектов)	Самостоятельная работа	Учебная практика	Производственная
1	2	3	4	5	6	7	8	9	10
ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09	Раздел 1. Порядок осуществление модификации информационных систем	122	56	112	112	-	10	-	-
ПК 5.1, ПК 5.2, ПК 5.3, ПК 5.4 ОК 01, ОК 02, ОК.04, ОК.09	Раздел 2. Основы цифровой экономики	36	12	36	36	-	0	-	-
	Учебная практика	36	36	-	-	-	-	36	-
	Производственная практика	72	72	-	-	-	-	-	72
	Промежуточная аттестация	20							
	Всего:	286	176	148	148	-	10	36	72

2.3. Содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, acad. ч / в том числе в форме практической подготовки, acad. ч	Код ПК, ОК
1	2	3	4
Раздел 1. Порядок осуществление модификации информационных систем		132/54	
МДК 13.01 Осуществление модификации информационных систем		132/54	
Тема 1.1. Разработка документации информационных систем	Содержание	10	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Основные понятия процесса проектирования автоматизированной информационной системы на основе анализа предметной области		
	Перечень и комплектность документов на информационные системы согласно ЕСПД и ЕСКД.		
	2.Задачи документирования		
	3. Предпроектная стадия разработки.		
	4. Техническое задание на разработку: основные разделы		
	5. Построение и оптимизация сетевого графика.		
	6. Проектная документация.		
	7. Техническая документация.		
	8. Отчётная документация		
	9. Пользовательская документация.		
	10. Назначение, виды и оформление сертификатов.		
	Практические занятия и лабораторные работы	28	
	1. Разработка технического задания.	6	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
2. Обеспечение надёжности функционирования системы	6		
3. Требования к программной документации	6		
4. Разработка отчётной документации.	4		
5. Разработка пользовательской документации.	6		

Тема 1.2. Отладка и тестирование информационных систем	Содержание	4	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Технологии отладки.		
	2. Виды тестирования.		
	3. Методы тестирования.		
	4. Верификация и валидация. Этапы и преимущества.		
	5. Оформление результатов тестирования.		
	Практические занятия и лабораторные работы	14	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	6. Разработка тестового сценария проекта.	4	
	7. Разработка тестовых пакетов.	2	
	8. Функциональное тестирование	2	
	9. Нагрузочное тестирование	2	
10. Стрессовое тестирование	2		
11. Конфигурационное тестирование.	2		
Тема 1.3. Система обеспечения качества информационных систем	Содержание	12	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Основные понятия качества информационной системы.		
	2. Национальный стандарт обеспечения качества автоматизированных информационных систем.		
	3. Международная система стандартизации и сертификации качества продукции.		
	4. Стандарты группы ISO.		
	5. Методы контроля качества в информационных системах.		
	6. Особенности контроля в различных видах систем.		
	7. Стратегия развития бизнес-процессов.		
	8. Обеспечение безопасности функционирования информационных систем		
	Практические занятия и лабораторные работы	36	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Построение модели управления качеством процесса изучения модуля.	4	
	2. Проектирование информационной системы для библиотеки.	2	
	3. Разработка информационной системы для библиотеки.	2	
	4. Тестирование информационной системы для библиотеки.	2	
	5. Проектирование информационной системы для торгового павильона.	4	
6. Разработка информационной системы для торгового павильона.	2		
7. Тестирование информационной системы торгового павильона.	2		

	8. Проектирование информационной системы для кинотеатра.	4	
	9. Разработка информационной системы для кинотеатра.	2	
	10. Тестирование информационной системы для кинотеатра.	2	
	11. Проектирование и разработка информационной системы для магазина строительных материалов.	4	
	12. Проектирование информационной системы для магазина строительных материалов.	2	
	13. Разработка информационной системы для магазина строительных материалов.	2	
	14. Создание программ по защите информации. Использование пароля с проверкой	2	
Тема 1.4. Оценка экономической эффективности информационных систем	Содержание	8	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Оценка экономической эффективности информационной системы.		
	2. Стоимостная оценка проекта.		
	3. Классификация типов оценок стоимости: оценка порядка величины.		
	4. Концептуальная оценка стоимости, предварительная оценка.		
	Практические занятия и лабораторные работы	8	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Расчёт и оценка экономической эффективности информационной системы.	4	
	2. Расчёт затрат на рекламу программного продукта	4	
Тематика самостоятельной учебной работы при изучении раздела 1		10	
1. Составление реферата на тему: «Техническое задание: основные разделы».			
2. Разработка презентации на тему: «Международная система стандартизации и сертификации качества продукции»			
3. Решение задачи своего варианта: Расчёт экономической эффективности информационной системы.			
Учебная практика Виды работ		-	
Производственная практика (по профилю специальности) Виды работ		-	
Промежуточная аттестация		10	
Раздел 2. Основы цифровой экономики		36 / 18	
МДК 13.02 Цифровая экономика в информационных системах		36 / 18	
	Содержание	4	

Тема 2.1. Цифровая экономика. Цели, задачи, базовые направления развития	1. Цели, задачи и риски развития цифровой экономики в России. Анализ текущего состояния развития цифровых технологий в РФ. Концепция цифровой экономики. Цифровая грамотность населения. Опорная инфраструктура и государственная поддержка.		ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	2 Технологическое развитие: исторические вехи и современность. Информационная экономика как основа развития цифровой экономики. Основные характеристики и возможности информационной (сетевой) экономики. Информация как производительная сила и стратегический ресурс. Модели информационной экономики. Принципы информационного общества. Структура современного общества. Производственные отношения. Экономическая сфера общества.		
	Практические занятия и лабораторные работы	8	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Освоение основных понятий цифровой экономики. Изучение нормативно-правового регулирования цифровой экономики в РФ	2	
	2. Анализ концепции развития государственных и муниципальных услуг	2	
	3. Экономическая информация. Экономические характеристики современного информационного общества.		
	4. Сканирование внешней среды. Субъектно-объектная модель информационного общества.	2	
	5. Предоставление государственных услуг Российской Федерации. Анализ концепции развития государственных и муниципальных услуг		
6. Рассмотрение свойств и особенностей цифровой экономики.	2		
7. Создание организационной структуры компании. Бизнес-процесс, клиент, сделка, материал, проект рекламной компании, сайт. Создание проекта рекламной компании			
Тема 2.2 Влияние цифровой трансформации и на экономику и бизнес	Содержание	4	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Новые экономические законы. Влияние информационной экономики на участников рынка (покупатели, производители, структура коммерческих отношений). Цифровая экономика как дальнейшее развитие новой (информационной) экономики. Ключевые тренды в цифровой экономике. Влияние цифровой трансформации на бизнес-среду.		
	2. Цифровая трансформация промышленности. Снижение издержек в цифровой экономике, цифровое пиратство, возможности ценовой дискриминации в цифровой экономике, проблемы раскрытия персональных данных. Перспективы развития проекта цифровой трансформации.		
	Практические занятия и лабораторные работы	8	ПК 5.1, ПК 5.2, ПК 5.3
	1. Характеристика цифровых технологий.	2	
2. Анализ перспектив развития цифровой экономики с помощью информационных сервисов.			

	3. Применение информационных сервисов в профессиональной деятельности. Поддержка IT-инфраструктуры.	2	ОК 01, ОК 02, ОК.04, ОК.09
	4. Применение информационных сервисов в профессиональной деятельности. Поддержка бизнес-приложений.		
	5. Применение информационных сервисов в профессиональной деятельности. Поддержка пользователей.	2	
	6. Использование информационных сервисов для анализа уровня цифровизации отраслей.		
	7. Использование перспективных цифровых технологий в деятельности компании.	2	
	8. Анализ уровня цифровизации деятельности компании.		
	9. Обзор онлайн решений управления компанией на рынке цифровых платформ. Выбор наиболее оптимальной для внедрения в деятельности компании.		
Тема 2.3 Основные технологические составляющие цифровой экономики	Содержание	4	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Блокчейн и криптовалюта.		
	2. Искусственный интеллект и машинное обучение. Анализ больших данных. Платформы цифровой экономики.		
	Практические занятия и лабораторные работы	2	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Сбор данных с интернет ресурсов. Статистический анализ больших данных.		
	2. Мониторинг социальных сетей.	2	
	3. Интернет вещей.		
Тема 2.4 Инструменты коммуникации в цифровой экономике	Содержание	2	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Информационно-телекоммуникационная инфраструктура цифровой экономики Электронное правительство.		
	2. Архитектура электронных услуг для граждан и бизнеса. Государственные информационные системы в социально-политической сфере.		
	Практические занятия и лабораторные работы	4	ПК 5.1, ПК 5.2, ПК 5.3
	1. Управление взаимоотношениями с клиентами CRM.		
	2. Управление Интернет маркетингом.	2	
	3. Управление проектами (PM)		

	4.Управление проектами (PM)		ОК 01, ОК 02, ОК.04, ОК.09
	5.Применение цифровых технологий на практике для выбранной организации.		
Тема 2.5 Информационная безопасность в цифровой экономике	Содержание	4	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
	1. Предмет и объект защиты. Цифровой этикет и цифровая гигиена.		
	2. Риски при работе с данными. Методы и средства защиты информации. Управление доступом. Идентификация и аутентификация.		
	3. Криптография и стеганография. Компьютерные вирусы антивирусная защита.		
Учебная практика Виды работ		-	
Производственная практика (по профилю специальности) Виды работ		-	
Промежуточная аттестация –		6	
Учебная практика по модулю Виды работ Разработка документации информационных систем. Отладка и тестирование информационных систем Система обеспечения качества информационных систем Основные технологические составляющие цифровой экономики Инструменты коммуникации в цифровой экономике Информационная безопасность в цифровой экономике		36	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09
Производственная практика по модулю Виды работ Подготовительный этап (инструктаж по технике безопасности) Ознакомление со структурой и характером деятельности предприятия; На примере одной подсистемы ИС разработать разделы проекта: Определение модулей, которые необходимо модифицировать и в каком направлении; Работа с программным обеспечением для анализа производительности и оптимизации работы информационной системы Работа со стандартами и эксплуатационной документацией; Анализ данных и составление отчётной документации по результатам анализа; Осуществление сопровождения и настройки информационной системы согласно технической документации;		72	ПК 5.1, ПК 5.2, ПК 5.3 ОК 01, ОК 02, ОК.04, ОК.09

<p>Оформление программной и технической документации с использованием стандартов оформления программной документации;</p> <p>Выполнение производственных заданий:</p> <ul style="list-style-type: none"> - разработка или модификация программ; - подготовка объекта автоматизации к вводу ИС в действие; - проведение предварительных испытаний; - проведение опытной эксплуатации; - проведение приёмочных испытаний; - документирование произведённых изменений; <p>Оформление отчёта о практике</p>		
Промежуточная аттестация (экзамен по модулю)	20	
Всего	286	

1. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение:

Лаборатории «Программного обеспечения и сопровождения компьютерных систем», оснащённая в соответствии с приложением 3 ОПОП-П.

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

1.2. Учебно-методическое обеспечение

3.2.1. Основные печатные издания

1. ГОСТ 34.201-2020. Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем. – М., Российский институт Стандартизации, 2021. – 12 с.

2. Рочев К.В. Информационные технологии. Анализ и проектирование информационных систем: учебное пособие / К.В. Рочев. – СПб.: Лань, 2022. – 128с.

Основные электронные издания

1. ГОСТ Р 51904-2002 Программное обеспечение встроенных систем // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс.]. – Режим доступа: <https://docs.cntd.ru/document/1200030195>, свободный.

2. ГОСТ Р ИСО/МЭК 12207-99. Информационная технология. Процессы жизненного цикла программных средств // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс.]. – Режим доступа: <https://docs.cntd.ru/document/1200009075#7D20K3>, свободный.

3.2.2. Дополнительные источники (при необходимости)

1. Гниденко И.Г. Технология разработки программного обеспечения: учебное пособие для среднего профессионального образования / И.Г. Гниденко, Ф.Ф. Павлов, Д.Ю. Федоров. – М.: Юрайт, 2023. – 235 с.

2. Соснин П.И. Архитектурное моделирование автоматизированных систем: учебник / П.И. Соснин. – СПб.: Лань, 2023. – 180 с.

3. Избачков Ю.С. Информационные системы: учебник / Ю.С. Избачков, В.Н. Петров, А.А. Васильев, И.С. Телина. – 3-е изд. — СПб.: Питер, 2011. — 544 с.

4. Рудаков А.В. Технология разработки программных продуктов. Практикум: учеб. пособие для студ. учреждений сред. проф. образования / А.В. Рудаков, Г.Н. Федорова. – 4-е изд., стер. – М.: Издательский центр «Академия», 2014. – 192 с.

5. Фуфаев Д.Э. Разработка и эксплуатация автоматизированных информационных систем: учебник / Д.Э. Фуфаев, Э.В. Фуфаев. – 3-е изд., перераб. – М.: Академия, 2014. – 304 с.

6. Сухомлинов А.И. Анализ и проектирование информационных систем: учебное пособие / А.И. Сухомлинов. – 2-е издание, испр. и доп. – Владивосток: Издательство Дальневосточного федерального университета, 2021. – 360 с.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код ПК, ОК	Критерии оценки результата (показатели освоенности компетенций)	Формы контроля и методы оценки
ОК. 01	Обучающийся распознает задачу и/или проблему в профессиональном и/или социальном контексте. Обучающийся анализирует и выделяет её составные части. Обучающийся определяет этапы решения задачи, составляет план действия, реализовывает составленный план, определяет необходимые ресурсы. Обучающийся выявляет и эффективно ищет информацию, необходимую для решения задачи и/или проблемы. Обучающийся владеет актуальными методами работы в профессиональной и смежных сферах. Обучающийся оценивает результат и последствия своих действий (самостоятельно или с помощью наставника)	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: -на практических занятиях; - при выполнении работ на различных этапах практики
ОК. 02	Обучающийся применяет современную научную профессиональную терминологию. Обучающийся определяет и выстраивает траектории профессионального развития и самообразования. Обучающийся определяет источники достоверной правовой информации	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: -на практических занятиях; - при выполнении работ на различных этапах практики
ОК. 04	Обучающийся организует работу коллектива и команды. Обучающийся взаимодействует с коллегами, руководством, клиентами в ходе профессиональной деятельности.	Экспертное наблюдение и оценка результатов формирования поведенческих навыков в ходе обучения
ОК. 09	Обучающийся понимает общий смысл чётко произнесённых высказываний на известные темы (профессиональные и бытовые), понимает тексты на базовые профессиональные темы. Обучающийся участвует в диалогах на знакомые общие и профессиональные темы. Обучающийся строит простые высказывания о себе и о	Оценка соблюдения правил оформления документов и построения устных сообщений на государственном языке Российской Федерации и иностранных языках

	своей профессиональной деятельности. Обучающийся кратко обосновывает и объясняет свои действия (текущие и планируемые). Обучающийся пишет простые связные сообщения на знакомые или интересующие профессиональные темы	
ПК 5.1	Обучающийся эффективно разрабатывает документацию, описывающую произведённые изменения в модуле, результативно проводит тестирование модифицированного модуля. Обучающийся демонстрирует соответствие общей стратегии развития системы техническому заданию.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: -на практических занятиях; - при выполнении работ на различных этапах практики. Решение практико-ориентированных ситуационных заданий.
ПК 5.2	Обучающийся эффективно использует различные методы и инструменты для оценки качества информационной системы. Обучающийся демонстрирует выполнение анализа по автоматизации бизнес-процессов, результативный анализ показателей экономической эффективности.	Экспертное наблюдение и оценка результатов формирования поведенческих навыков в ходе обучения
ПК 5.3	Обучающийся проводит эффективное планирование своей деятельности по сбору данных для функционирования информационной системы, грамотное использование полученных данных для оптимизации работы системы. Обучающийся проводит работу с различными видами проектной документации.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: -на практических занятиях; - при выполнении работ на различных этапах практики. Решение практико-ориентированных ситуационных заданий.
ПК 5.4	Обучающийся выявляет основные тенденции в развитии современной мировой экономики, анализирует	Контрольные работы, зачёты, экзамены. Интерпретация

	<p>последствия управленческих решений в сфере бизнеса в условиях цифровизации экономики.</p> <p>Обучающийся осуществляет поиск, анализ и управление информацией в цифровой среде.</p> <p>Обучающийся применяет информационные сервисы в профессиональной деятельности, демонстрирует знания основных технологических составляющих цифровой экономики, инструментов коммуникации, методов и средств защиты информации</p>	<p>результатов выполнения практических и лабораторных заданий, оценка решения ситуационных задач, оценка тестового контроля.</p>
--	--	--

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.06 ОСУЩЕСТВЛЕНИЕ ИНТЕГРАЦИИ ПРОГРАММНЫХ МОДУЛЕЙ»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМд.05 ОСУЩЕСТВЛЕНИЕ ИНТЕГРАЦИИ ПРОГРАММНЫХ МОДУЛЕЙ

Цель и результаты освоения профессионального модуля

Часть данной программы может быть реализована с применением дистанционных образовательных технологий.

В результате изучения профессионального модуля студент должен освоить основной вид деятельности
Осуществление интеграции программных модулей и соответствующие ему общие компетенции и профессиональные компетенции:

1.1.1. Перечень общих компетенций:

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 5	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 9	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 11	Планировать предпринимательскую деятельность в профессиональной сфере

Перечень профессиональных компетенций

Виды деятельности	Код и наименование компетенции	Код	Показатели освоения компетенции
ВД. 06 Осуществление интеграции программных модулей и соответствующее ему общие компетенции и профессиональные компетенции	ПК 6.1 Формализация и алгоритмизация поставленных задач для разработки программного кода		Навыки:
		Н.01	Составление формализованных описаний решений поставленных задач в соответствии с требованиями технического задания или внутренних документов организации
		Н.02	Разработка алгоритмов решения поставленных задач в соответствии с требованиями технического задания или внутренних документов организации
		Н.03	Проверка корректности алгоритмов решения поставленных задач
		Н.04	Оценка и согласование сроков выполнения поставленных задач
			Умения:
		У.01	Использовать методы и приемы формализации поставленных задач
		У.02	Использовать методы и приемы алгоритмизации поставленных задач
		У.03	Использовать программное обеспечение для графического отображения алгоритмов
		У.04	Применять алгоритмы решения типовых задач в соответствующих областях
		У.05	Осуществлять коммуникации с заинтересованными сторонами
			Знания:
		3.01	Методы и приемы формализации поставленных задач
		3.02	Языки формализации функциональных спецификаций
		3.03	Методы и приемы алгоритмизации поставленных задач
			3.04

		3.05	Алгоритмы решения типичных задач, области и способы их применения
		3.06	Методы и приемы формализации поставленных задач
	ПК 6.2. Написание программного кода с использованием языков программирования, определения и манипулирования данными в базах данных	Н.01	Создание программного кода в соответствии с техническим заданием (готовыми спецификациями)
		Н.02	Оптимизация программного кода с использованием специализированных программных средств
		Н.03	Оценка и согласование сроков выполнения поставленных задач
			Умения:
		У.01	Применять выбранные языки программирования для написания программного кода
		У.02	Использовать выбранную среду программирования и средства системы управления базами данных
		У.03	Использовать возможности имеющейся технической и/или программной архитектуры для написания программного кода
		У.04	Осуществлять коммуникации с заинтересованными сторонами
			Знания:
		3.01	Синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования
		3.02	Методологии разработки компьютерного программного обеспечения
		3.03	Методологии и технологии проектирования и использования баз данных
		3.04	Технологии программирования
			Особенности выбранной среды программирования и системы управления базами данных
	3.05	Компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними	

		3.06	Синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования
ПК.6.3. Оформление программного кода в соответствии с установленными требованиями		Н.01	Приведение наименований переменных, функций, классов, структур данных и файлов в соответствии с нормативно-техническими документами (стандартами и регламентами), определяющими требования к оформлению программного кода
		Н.02	Структурирование исходного программного кода в соответствии с нормативно-техническими документами (стандартами и регламентами), определяющими требования к оформлению программного кода
		Н.03	Комментирование и разметка программного кода в соответствии с нормативно-техническими документами (стандартами и регламентами), определяющими требования к оформлению программного кода
		Н.04	Форматирование исходного программного кода в соответствии с нормативно-техническими документами (стандартами и регламентами), определяющими требования к оформлению программного кода
		Н.05	Оформление технической документации на компьютерное программное обеспечение по заданному стандарту или шаблону
			Умения:
		У.01	Применять нормативно-технические документы (стандарты и регламенты), определяющие требования к оформлению программного кода
		У.02	Применять инструментарий для создания и актуализации исходных текстов программ
		У.03	Применять заданные стандарты и шаблоны для составления и оформления технической документации
		У.04	Осуществлять коммуникации с заинтересованными сторонами
			Знания:

		3.01	Инструментарий для создания и актуализации исходных текстов программ
		3.02	Методы повышения читаемости программного кода
		3.03	Системы кодировки символов, форматы хранения исходных текстов программ
		3.04	Нормативно-технические документы (стандарты и регламенты), определяющие требования к оформлению программного кода
		3.05	Основные стандарты оформления технической документации на компьютерное программное обеспечение
	ПК 6.4. Работа с системой управления версиями программного кода	H.01	Регистрация изменений исходного текста программного кода в системе управления версиями
		H.02	Слияние, разделение и сравнение исходных текстов программного кода
		H.03	Сохранение сделанных изменений программного кода в соответствии с регламентом управления версиями
			Умения:
		У.01	Использовать выбранную систему управления версиями
		У.02	Использовать вспомогательные инструментальные программные средства для обработки исходного текста программного кода
		У.03	Выполнять действия, соответствующие установленному регламенту используемой системы управления версиями
			Знания:
		3.01	Возможности используемой системы управления версиями и вспомогательных инструментальных программных средств
		3.02	Установленный регламент использования системы управления версиями
	ПК 6.5. Проверка и отладка	H.01	Анализ и проверка исходного программного кода
		H.02	Отладка программного кода на уровне программных модулей

	программного кода	H.03	Отладка программного кода на уровне межмодульных взаимодействий и взаимодействий с окружением
			Умения:
		У.01	Выявлять ошибки в программном коде
		У.02	Применять методы и приемы отладки программного кода
		У.03	Интерпретировать сообщения об ошибках, предупреждения, записи технологических журналов
		У.04	Применять современные компиляторы, отладчики и оптимизаторы программного кода
			Знания:
		3.01	Методы и приемы отладки программного кода
		3.02	Типы и форматы сообщений об ошибках, предупреждений
		3.3	Способы использования технологических журналов, форматы и типы записей журналов
		3.04	Современные компиляторы, отладчики и оптимизаторы программного кода
		3.05	Сообщения о состоянии аппаратных средств
	ПК 7.1. Разработка процедур проверки работоспособности и измерения характеристик к компьютерного программного обеспечения	H.01	Разработка процедуры проверки работоспособности компьютерного программного обеспечения
		H.02	Разработка процедуры сбора диагностических данных проверки работоспособности компьютерного программного обеспечения
		H.03	Разработка процедуры измерения требуемых характеристик компьютерного программного обеспечения
H.04		Оформление технической документации на компьютерное программное обеспечение по заданному стандарту или шаблону	
H.05		Оценка и согласование сроков выполнения поставленных задач	
		Умения:	

		У.01	Писать программный код процедур проверки работоспособности компьютерного программного обеспечения на выбранном языке программирования
		У.02	Использовать выбранную среду программирования для разработки процедур проверки работоспособности компьютерного программного обеспечения
		У.03	Применять заданные стандарты и шаблоны для составления и оформления технической документации
			Знания:
		3.01	Методы автоматической и автоматизированной проверки работоспособности компьютерного программного обеспечения
		3.02	Основные виды диагностических данных проверки работоспособности компьютерного программного обеспечения и способы их представления
		3.03	Языки, утилиты и среды программирования и средства пакетного выполнения процедур
			Типовые метрики компьютерного программного обеспечения
		3.04	Основные методы измерения и оценки характеристик компьютерного программного обеспечения
		3.05	Основные стандарты оформления технической документации на компьютерное программное обеспечение
	ПК 7.2. Разработка тестовых наборов данных для проверки работоспособности компьютерного программного обеспечения	Н.01	Подготовка тестовых наборов данных в соответствии с выбранной методикой тестирования компьютерного программного обеспечения
		Н.02	Оценка и согласование сроков выполнения поставленных задач
			Умения:
		У.01	Разрабатывать и оформлять контрольные примеры для проверки работоспособности компьютерного программного обеспечения
		У.02	Разрабатывать процедуры генерации тестовых наборов данных с заданными характеристиками

		У.03	Подготавливать наборы данных, используемых в процессе проверки работоспособности компьютерного программного обеспечения
		У.04	Использовать командные средства разработки компьютерного программного обеспечения
		У.05	Осуществлять коммуникации с заинтересованными сторонами
			Знания:
		3.01	Методы создания и документирования контрольных примеров и тестовых наборов данных
		3.02	Правила, алгоритмы и технологии создания тестовых наборов данных
	ПК 7.3 . Проверка работоспособности компьютерного программного обеспечения	Н.01	Проверка работоспособности компьютерного программного обеспечения на основе разработанных тестовых наборов данных
		Н.02	Оценка соответствия компьютерного программного обеспечения требуемым характеристикам
		Н.03	Сбор и анализ полученных результатов проверки работоспособности компьютерного программного обеспечения
		Н.04	Оценка и согласование сроков выполнения поставленных задач
			Умения:
		У.01	Применять методы и средства проверки работоспособности компьютерного программного обеспечения
		У.02	Интерпретировать диагностические данные проверки работоспособности компьютерного программного обеспечения
		У.03	Анализировать значения полученных характеристик компьютерного программного обеспечения
		У.04	Документировать результаты проверки работоспособности компьютерного программного обеспечения

		3.01	Методы и средства проверки работоспособности компьютерного программного обеспечения
		3.02	Среды проверки работоспособности и отладки компьютерного программного обеспечения
		3.03	Государственные стандарты испытания автоматизированных систем
		3.04	Руководящие документы по стандартизации требований к документам автоматизированных систем
ПК 7.4 Рефакторинг, оптимизация и инспекция программного кода		Н.01	Анализ программного кода на соответствие требованиям по читаемости и производительности
		Н.02	Инспекция программного кода для поиска не обнаруженных на ранних стадиях разработки компьютерного программного обеспечения ошибок и критических мест
		Н.03	Внесение изменений в программный код и проверка его работоспособности
			Умения:
		У.01	Применять методы, средства рефакторинга, оптимизации и инспекции программного кода
		У.02	Применять инструментальные средства коллективной работы над программным кодом
		У.03	Публиковать результаты рефакторинга, оптимизации и инспекции в коллективной базе знаний
		У.04	Использовать систему управления версиями для регистрации произведенных изменений
		У.05	Осуществлять коммуникации с заинтересованными сторонами
			Знания:
		3.01	Методы и средства рефакторинга, оптимизации и инспекции программного кода
		3.02	Языки программирования и среды разработки
		3.03	Нормативно-технические документы (стандарты и регламенты), регламентирующие требования к программному коду, порядок отражения изменений в системе управления версиями, порядок отражения

		результатов рефакторинга, оптимизации и инспекции в коллективной базе знаний
ПК 7.5. Исправление дефектов программного кода, зафиксированных в базе данных дефектов	H.01	Воспроизведение дефектов программного кода, зафиксированных в базе данных дефектов
	H.02	Установление причин возникновения дефектов программного кода
	H.03	Внесение изменений в программный код для устранения выявленных дефектов
	H.04	Оценка и согласование сроков выполнения поставленных задач
	H.05	Воспроизведение дефектов программного кода, зафиксированных в базе данных дефектов
		Умения:
	У.01	Применять методы и приемы отладки дефектного программного кода
	У.02	Интерпретировать сообщения, предупреждения, записи технологических журналов об ошибках, возникающих при выполнении дефектного кода
	У.03	Осуществлять коммуникации с заинтересованными сторонами
		Знания:
	З.01	Методы и приемы отладки программного кода
	З.02	Типичные ошибки, возникающие при разработке компьютерного программного обеспечения, методы их диагностики и исправления
	ПК 7.6 Осуществление сборки однородных программных модулей в программный проект	H.01
H.02		Проверка работоспособности собранного программного проекта
H.03		Внесение изменений в процедуру сборки однородных (однойязыковых) программных модулей в программный проект
		Умения:

		У.01	Выполнять процедуры сборки однородных (одноязыковых) программных модулей в программный проект в средах разработки компьютерного программного обеспечения
		У.02	Производить настройки параметров программного проекта и осуществлять запуск процедур сборки
		У.03	Проводить проверку работоспособности программного проекта
		У.04	Документировать произведенные действия, выявленные проблемы и способы их устранения
		У.05	Создавать резервные копии программного проекта и данных, выполнять восстановление, обеспечивать целостность программного проекта и данных
		У.06	Выполнять процедуры сборки однородных (одноязыковых) программных модулей в программный проект в средах разработки компьютерного программного обеспечения
			Знания:
		3.01	Методы и средства сборки модулей в программный проект в средах разработки компьютерного программного обеспечения
		3.02	Возможности настройки программного проекта в средах разработки компьютерного программного обеспечения
		3.03	Интерфейсы взаимодействия внутренних модулей программного проекта
	ПК 8.1. Разработка процедур интеграции программных модулей	Н.01	Анализ и выявление проблем сопряжения неоднородных модулей и компонентов компьютерного программного обеспечения
		Н.02	Разработка и документирование программных интерфейсов
		Н.03	Разработка процедур сборки модулей и компонентов компьютерного программного обеспечения
		Н.04	Разработка процедур развертывания и обновления компьютерного программного обеспечения

		H.05	Разработка процедур миграции и преобразования (конвертации) данных
		H.05	Оформление технической документации на компьютерное программное обеспечение по заданному стандарту или шаблону
		H.06	Оценка и согласование сроков выполнения поставленных задач
		H.07	Анализ и выявление проблем сопряжения неоднородных модулей и компонентов компьютерного программного обеспечения
			Умения:
		У.01	Писать программный код процедур интеграции программных модулей
		У.02	Использовать выбранную среду программирования для разработки процедур интеграции программных модулей
		У.03	Применять методы и средства сборки модулей и компонентов компьютерного программного обеспечения, разработки процедур для развертывания компьютерного программного обеспечения, миграции и преобразования данных, создания программных интерфейсов
		У.04	Применять заданные стандарты и шаблоны для составления и оформления технической документации
			Знания:
		3.01	Методы и средства сборки модулей и компонентов компьютерного программного обеспечения
		3.02	Интерфейсы взаимодействия с внешней средой
		3.03	Интерфейсы взаимодействия внутренних модулей системы
		3.04	Методы и средства разработки процедур для развертывания компьютерного программного обеспечения
		3.05	Методы и средства миграции и преобразования данных

		3.06	Языки, утилиты и среды программирования, средства пакетного выполнения процедур
		3.07	Основные стандарты оформления технической документации на компьютерное программное обеспечение
		3.08	Методы и средства сборки модулей и компонентов компьютерного программного обеспечения
	ПК 8.2 Осуществление интеграции программных модулей и компонентов и проверки работоспособности выпусков программного продукта	H.01	Сборка программных модулей и компонентов в программный продукт
		H.02	Подключение программного продукта к компонентам внешней среды
		H.03	Проверка работоспособности выпусков программного продукта
		H.04	Внесение изменений в процедуры сборки модулей и компонентов компьютерного программного обеспечения, развертывания компьютерного программного обеспечения, миграции и преобразования данных
			Умения:
У.01		Выполнять процедуры сборки программных модулей и компонентов в программный продукт	
У.02		Производить настройки параметров программного продукта и осуществлять запуск процедур сборки	
У.03		Проводить проверку работоспособности программного продукта	
У.04		Документировать произведенные действия, выявленные проблемы и способы их устранения	
У.05		Использовать командные средства разработки компьютерного программного обеспечения	
У.06		Создавать резервные копии программ и данных, выполнять восстановление, обеспечивать целостность программного продукта и данных	
У.07		Выполнять процедуры сборки программных модулей и компонентов в программный продукт	
	Знания:		

		3.01	Методы и средства сборки и интеграции программных модулей и компонентов
		3.02	Интерфейсы взаимодействия программного продукта с внешней средой
		3.03	Интерфейсы взаимодействия внутренних модулей программного продукта
		3.04	Методы и средства проверки работоспособности выпусков программных продуктов
		3.05	Языки, утилиты и среды программирования, средства пакетного выполнения процедур

Количество часов, отводимое на освоение профессионального модуля

Всего часов:	206
на освоение МДК	134
учебную	0
производственную	72

2. СТРУКТУРА и содержание профессионального модуля

2.1. Структура профессионального модуля ПМ.06. Осуществление интеграции программных модулей

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, час.					
			Обучение по МДК				Практики	
			Самостоятельная работа	Всего	Лабораторных и практических занятий	Курсовых работ (проектов)	Учебная	Производственная
ПК 6.1-6.5. ПК 7.1-7.6.	Раздел 1. Технология разработки программного обеспечения	110	6	104	52			
ПК 7.1-7.2	Раздел 2. Инструментальные средства разработки программного обеспечения	150	4	74	36		72	
ПК 6.1-6.5. ПК 7.1-7.6 ПК 8.1-8.2	Производственная практика (по профилю специальности), часов	72						72
	Промежуточная аттестация	30						

	Bcero:	362	10	178	88		72	72
--	--------	-----	----	-----	----	--	----	----

2.2. Тематический план и содержание профессионального модуля ПМд.06. Осуществление интеграции программных модулей

Программист

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект)	Объем в часах
1	2	3
Раздел 1. Разработка программного обеспечения		
МДК. 06.01 Технология разработки программного обеспечения		132
Тема 2.1.1 Основные понятия и стандартизация требований к программному обеспечению	Содержание	32
	Понятия требований, классификация, уровни требований. Методологии и стандарты, регламентирующие работу с требованиями.	16
	Современные принципы и методы разработки программных приложений.	
	Методы организации работы в команде разработчиков. Системы контроля версий	
	Основные подходы к интегрированию программных модулей.	
	Стандарты кодирования.	
	В том числе практических занятий и лабораторных работ	16
Практическое занятие «Анализ предметной области»	4	

	Практическое занятие «Разработка и оформление технического задания»	4
	Практическое занятие «Построение архитектуры программного средства»	4
	Практическое занятие «Изучение работы в системе контроля версий»	4
Тема 2.1.2. Описание и анализ требований. Диаграммы IDEF	Содержание	36
		16
	Описание требований: унифицированный язык моделирования – краткий словарь.	2
	Диаграммы UML.	4
	Сущности UML (Структурные, Поведенческие, Поведенческие).	2
	Связи UML .	2
	Описание требований (спецификация).	2
	Оформление требований.	4
	Анализ требований.	4
	Анализ стратегии выбора решения.	2
	В том числе практических занятий и лабораторных работ	20
	Лабораторная работа «Построение диаграммы Вариантов использования и диаграммы. Последовательности»	4
	Лабораторная работа «Построение диаграммы Кооперации и диаграммы Развертывания»	4

	Лабораторная работа «Построение диаграммы Деятельности, диаграммы Состояний и диаграммы Классов»	4
	Лабораторная работа «Построение диаграммы компонентов»	4
	Лабораторная работа «Построение диаграмм потоков данных»	4
Тема 2.1.3. Оценка качества программных средств	Содержание	40
	Цели и задачи и виды тестирования.	4
	Стандарты качества программной документации.	
	Меры и метрики.	4
	Тестовое покрытие.	
	Тестовый сценарий.	4
	Тестовый пакет.	
	Анализ спецификаций.	6
	Верификация и аттестация программного обеспечения.	
	В том числе практических занятий и лабораторных работ	22
	Лабораторная работа «Разработка тестового сценария»	4
	Лабораторная работа «Оценка необходимого количества тестов»	4
	Лабораторные работы «Разработка тестовых пакетов»	4
	Лабораторные работы «Оценка программных средств с помощью метрик»	4

	Лабораторные работы «Инспекция программного кода на предмет соответствия стандартам кодирования»	6
Промежуточная аттестация)		10

Раздел 2. Средства разработки программного обеспечения		
МДК.06.02 Инструментальные средства разработки программного обеспечения		36
Тема 2.2.1 Современные технологии и инструменты интеграции.	Содержание	12
	Понятие репозитория проекта, структура проекта.	
	Виды, цели и уровни интеграции программных модулей. Автоматизация бизнес-процессов.	
	Выбор источников и приемников данных, сопоставление объектов данных.	
	Транспортные протоколы. Стандарты форматирования сообщений.	
	Организация работы команды в системе контроля версий.	
	В том числе практических занятий и лабораторных работ	4
	Лабораторная работа «Разработка структуры проекта»	
	Лабораторная работа «Разработка модульной структуры проекта (диаграммы модулей)»	
	Лабораторная работа «Разработка перечня артефактов и протоколов проекта»	

	Лабораторная работа «Настройка работы системы контроля версий (типов импортируемых файлов, путей, фильтров и др. параметров импорта в репозиторий)»	
	Лабораторная работа «Разработка и интеграция модулей проекта (командная работа)»	
	Лабораторная работа «Отладка отдельных модулей программного проекта»	
	Лабораторная работа «Организация обработки исключений»	
Тема 2.2.2 Инструментарий тестирования и анализа качества программных средств	Содержание	
	Отладка программных продуктов. Инструменты отладки. Отладочные классы.	12
	Ручное и автоматизированное тестирование. Методы и средства организации тестирования.	
	Инструментарии анализа качества программных продуктов в среде разработки.	
	Обработка исключительных ситуаций. Методы и способы идентификации сбоев и ошибок.	
	Выявление ошибок системных компонентов.	
	В том числе практических занятий и лабораторных работ	8
	Лабораторная работа «Применение отладочных классов в проекте»	
	Лабораторная работа «Отладка проекта»	
	Лабораторная работа «Инспекция кода модулей проекта»	
	Лабораторная работа «Тестирование интерфейса пользователя средствами инструментальной среды разработки»	
	Лабораторная работа «Разработка тестовых модулей проекта для тестирования отдельных модулей»	

	Лабораторная работа «Выполнение функционального тестирования»	
	Лабораторная работа «Тестирование интеграции»	
	Лабораторная работа «Документирование результатов тестирования»	

Учебная практика	<p>Методы организации работы в команде разработчиков. Системы контроля версий Основные подходы к интегрированию программных модулей. Стандарты кодирования. Диаграммы UML. Сущности UML (Структурные, Поведенческие, Поведенческие). Связи UML . Описание требований (спецификация). Оформление требований. Анализ требований. Анализ стратегии выбора решения. Стандарты качества программной документации. Меры и метрики. Тестовое покрытие. Тестовый сценарий. Тестовый пакет. Анализ спецификаций. Верификация и аттестация программного обеспечения.</p>	36
Производственная практика	<p>Выбор источников и приемников данных, сопоставление объектов данных. Транспортные протоколы. Стандарты форматирования сообщений. Организация работы команды в системе контроля версий. Разработка структуры проекта Разработка модульной структуры проекта (диаграммы модуля) Разработка перечня артефактов и протоколов проекта Настройка работы системы контроля версий (типов импортируемых файлов, путей, фильтров и др. параметров импорта в репозиторий) Разработка и интеграция модулей проекта (командная работа) Отладка отдельных модулей программного проекта Организация обработки исключений Отладка программных продуктов. Инструменты отладки. Отладочные классы.</p>	72

	<p>Ручное и автоматизированное тестирование. Методы и средства организации тестирования. Инструментарии анализа качества программных продуктов в среде разработке. Обработка исключительных ситуаций. Методы и способы идентификации сбоев и ошибок. Выявление ошибок системных компонентов. Применение отладочных классов в проекте Отладка проекта Инспекция кода модулей проекта Тестирование интерфейса пользователя средствами инструментальной среды разработки Разработка тестовых модулей проекта для тестирования отдельных модулей Выполнение функционального тестирования Тестирование интеграции Документирование результатов тестирования</p>	
--	--	--

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Лаборатория «Программного обеспечения и сопровождения компьютерных систем»:

12-15 компьютеров обучающихся и 1 компьютер преподавателя (аппаратное обеспечение: оперативная память объемом не менее 1 ГБ, жесткие диски общим объемом не менее 80 Г);

Проектор и экран;

Маркерная доска;

Программное обеспечение общего и профессионального назначения, в том числе включающее в себя следующее ПО: EclipseIDEforJavaEEDevelopers, .NETFrameworkJDK 8, NetBeans, AndroidStudio, IntelliJIDEA.

3.2. Информационное обеспечение реализации программы

3.2.1. Электронные издания (электронные ресурсы)

1. От модели объектов - к модели классов. Единое окно доступа к образовательным ресурсам.
http://real.tepkom.ru/Real_OM-СМ_A.asp

<https://htmlacademy.ru/> HTML Academy – электронный портал изучения веб-верстки (HTML/CSS)

<http://htmlbook.ru/> – портал-справочник о HTML/CSS

<https://learn.javascript.ru/> - Курсы javascript от Ильи Кантора

<http://java-course.ru> – изучение языка программирования Java и объектно-ориентированного программирования

5. Долженко, А.И. Технологии командной разработки программного обеспечения информационных систем / А.И. Долженко. – 2-е изд., исправ. – Москва : Национальный Открытый Университет «ИНТУИТ», 2019. – 301 с. : схем., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=428801>

– Библиогр. в кн. – Текст : электронный.

6. Беспалов, Д.А. Операционные системы реального времени и технологии разработки кроссплатформенного программного обеспечения : учебное пособие : [16+] / Д.А. Беспалов, С.М. Гушанский, Н.М. Коробейникова ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2021. – Ч. 1. – 140 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=577698> – Библиогр. в кн. – ISBN 978-5-9275-3367-1. – Текст : электронный

7Мейер, Б. Объектно-ориентированное программирование и программная инженерия / Б. Мейер. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2021. – 286 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=429034>). – Текст : электронный.

8Смирнов, А.А. Прикладное программное обеспечение : учебное пособие : [16+] / А.А. Смирнов. – Москва ; Берлин : Директ-Медиа, 2021. – 358 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=457616> – Библиогр. в кн. – ISBN 978-5-4475-8780-2. – DOI 10.23681/457616. – Текст : электронный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
Раздел 1. Разработка программного обеспечения		
<p>ПК 6.1-6.5. ПК 7.1-7.6.</p>	<p>Оценка «отлично» - разработан и обоснован вариант интеграционного решения с помощью графических средств среды разработки, указано хотя бы одно альтернативное решение; бизнес-процессы учтены в полном объеме; вариант оформлен в полном соответствии с требованиями стандартов; результаты верно сохранены в системе контроля версий.</p> <p>Оценка «хорошо» - разработана и прокомментирована архитектура варианта интеграционного решения с помощью графических средств, учтены основные бизнес-процессы; вариант оформлен в соответствии с требованиями стандартов; результаты сохранены в системе контроля версий.</p> <p>Оценка «удовлетворительно» - разработана и архитектура варианта интеграционного решения с помощью графических средств, учтены основные бизнес-процессы с незначительными упущениями; вариант оформлен в соответствии с требованиями стандартов с некоторыми отклонениями; результат сохранен в системе контроля версий.</p>	<p>Экзамен/зачет в форме собеседования:</p> <p>- практическое задание по формированию требований к программным модулям в соответствии с техническим заданием.</p> <p>Защита отчетов по практическим и лабораторным работам.</p> <p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики</p>
Раздел модуля 2 Средства разработки программного обеспечения		
ПК 8.1-8.2	<p>Оценка «отлично» - в системе контроля версий выбрана верная версия проекта, проанализирована его архитектура, архитектура доработана для интеграции нового модуля; выбраны способы форматирования данных и организована их постобработка, транспортные протоколы и форматы сообщений обновлены (при необходимости); протестирована интеграция модулей проекта и выполнена отладка проекта с применением инструментальных средств среды; выполнена доработка модуля и дополнительная обработка</p>	<p>Экзамен/зачет в форме собеседования:</p> <p>практическое задание по обеспечению интеграции заданного модуля в предложенный программный проект</p>

	<p>исключительных ситуаций в том числе с созданием классов-исключений (при необходимости); определены качественные показатели полученного проекта; результат интеграции сохранен в системе контроля версий.</p> <p>Оценка «хорошо» - в системе контроля версий выбрана верная версия проекта, его архитектура доработана для интеграции нового модуля; выбраны способы форматирования данных и организована их постобработка, транспортные протоколы и форматы сообщений обновлены (при необходимости); выполнена отладка проекта с применением инструментальных средств среды; выполнена доработка модуля и дополнительная обработка исключительных ситуаций (при необходимости); определены качественные показатели полученного проекта; результат интеграции сохранен в системе контроля версий.</p> <p>Оценка «удовлетворительно» - в системе контроля версий выбрана верная версия проекта, его архитектура доработана для интеграции нового модуля; выбраны способы форматирования данных и организована их постобработка, форматы сообщений обновлены (при необходимости); выполнена отладка проекта с применением инструментальных средств среды; выполнена доработка модуля (при необходимости); результат интеграции сохранен в системе контроля версий.</p>	<p>Защита отчетов по практическим и лабораторным работам</p> <p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики</p>
<p>ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.</p>	<p>обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;</p> <p>- адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач</p>	<p>Экспертное наблюдение за выполнением работ</p>
<p>ОП 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.</p>	<p>- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач</p>	
<p>ОК 03. Планировать и реализовывать собственное</p>	<p>- демонстрация ответственности за принятые решения</p>	

профессиональное и личностное развитие.	- обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействовать с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Демонстрировать грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- эффективность использовать средств физической культуры для сохранения и укрепления здоровья при выполнении профессиональной деятельности.	

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