

приложение 1.1  
к ОПОП по специальности  
10.02.05 Обеспечение информационной  
безопасности автоматизированных систем

**АДАптиРОВАННАЯ РАБОЧАЯ ПРОГРАММА**  
**ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 ЭКСПЛУАТАЦИЯ**  
**АВТОМАТИЗИРОВАННЫХ**  
**(ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**  
**для обучающихся с расстройством аутистического спектра**

## **СОДЕРЖАНИЕ**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА АДАПТИРОВАННОЙ 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 АДАПТИРОВАННОЙ 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:

<b>Код</b>	<b>Наименование видов деятельности и профессиональных компетенций</b>
<b>ВД 1</b>	<b>Эксплуатация автоматизированных (информационных) систем в защищенном исполнении</b>
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:**

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

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

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках

1.1.3. В результате освоения профессионального модуля студент должен:

<b>Иметь практический опыт</b>	<ul style="list-style-type: none"><li>– установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем;</li><li>– администрирования автоматизированных систем в защищенном исполнении;</li><li>– эксплуатации компонентов систем защиты информации автоматизированных систем;</li><li>– диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении</li></ul>
<b>уметь</b>	<ul style="list-style-type: none"><li>– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;</li><li>– организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;</li><li>– осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;</li><li>– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы</li><li>– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;</li><li>– обеспечивать работоспособность, обнаруживать и устранять неисправности</li></ul>
<b>знать</b>	<ul style="list-style-type: none"><li>– состав и принципы работы автоматизированных систем, операционных систем и сред;</li><li>– принципы разработки алгоритмов программ, основных приемов программирования;</li><li>– модели баз данных;</li><li>– принципы построения, физические основы работы периферийных устройств;</li><li>– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;</li><li>– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;</li><li>– принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.</li></ul>

## **1.2. Количество часов, отводимое на освоение профессионального модуля**

Всего 832 час, из них

на освоение МДК – 598 часов, в том числе

промежуточная аттестация – 54 часа,

производственная практика – 216 часов.

**МДК 01.01** Операционные системы - 96 часов

в том числе самостоятельная работа - 9 часов;

консультации - 9 часов;

практика производственная 36 часов.

**МДК 01.02** Базы данных - 132 часов

в том числе самостоятельная работа - 9 часов;

консультации - 9 часов;

производственная практика - 36 часов.

**МДК 01.03** Сети и системы передачи информации - 42 часа

в том числе самостоятельная работа - 4 часа;

консультации - 4 часа;

производственная практика - 36 часов.

**МДК 01.04** Эксплуатация автоматизированных (информационных) систем в защищенном исполнении - 164 часа

в том числе самостоятельная работа - 9 часов;

консультации - 9 часов;

экзамен по МДК 01.04 – 18 ч

**МДК 01.05** Эксплуатация компьютерных сетей - 164 часа

в том числе самостоятельная работа - 9 часов;

консультации - 9 часов;

производственная практика - 54 часа

экзамен по МДК 01.05 – 18 ч

**Экзамен по профессиональному модулю 18 часов.**

## 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.					Промежуточная аттестация
			Обучение по МДК, в час.			Практики		
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	Самостоятельная/консультации			
ПК 1.1-1.4 ОК 1-9	<b>Раздел 1.</b> МДК 01.01 Операционные системы	<b>132</b>	96	46	9/9	0	36	0
ПК 1.1-1.4 ОК 1-9	<b>Раздел 2.</b> МДК 01.02 Базы данных	<b>168</b>	132	68	9/9	0	36	0
ПК 1.1-1.4 ОК 1-9	<b>Раздел 3.</b> МДК 01.03 Сети и системы передачи информации	<b>78</b>	42	20	4/4	0	36	0
ПК 1.1-1.4 ОК 1-9	<b>Раздел 4.</b> МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	<b>218</b>	164	48	9/9	0	54	18
ПК 1.1-1.4 ОК 1-9	<b>Раздел 5.</b> МДК 01.05 Эксплуатация компьютерных систем	<b>218</b>	164	82	9/9	0	54	18
ПК 1.1-1.4 ОК 1-9	Экзамен по профессиональному модулю	<b>18</b>	-	-	-	-	-	-
	<b>Всего:</b>	<b>832</b>	<b>598</b>	264	80	-	<b>216</b>	<b>36</b>

## 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	
<b>РАЗДЕЛ 1</b>		<b>132</b>	
<b>МДК.01.01 Операционные системы</b>			
<b>Раздел 1. Элементы теории операционных систем. Свойства операционных систем</b>			
<b>Тема 1.1.</b> Основы теории операционных систем	<b>Содержание</b>	<b>2</b>	
	Определение операционной системы. Основные понятия. История развития операционных систем. ТЗ.1 Виды операционных систем. Классификация операционных систем по разным признакам. ТЗ.2 Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.	<b>2</b>	
<b>Тема 1.2.</b> Машинно-зависимые и машинно-независимые свойства операционных систем	<b>Содержание</b>	<b>2</b>	
	ТЗ.3 Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС.	<b>2</b>	
	Переносимость ОС. Машинно-зависимые модули ОС. ТЗ.4 Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.	<b>2</b>	
	Работа с файлами. ТЗ.5 Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.		
	<b>Тематика практических занятий</b>		
	ПЗ.1 Виртуальные машины. Создание, модификация, работа	<b>2</b>	
	ПЗ. 2 Установка ОС	<b>2</b>	
	ПЗ.3 Создание и изучение структуры разделов жесткого диска	<b>2</b>	
ПЗ. 4 Операции с файлами	<b>2</b>		
	<b>Содержание</b>	<b>2</b>	

<b>Тема 1.3.</b> Модульная структура	Экзоядро. ТЗ.6 Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме.	
--------------------------------------	---	--

операционных систем, пространство пользователя	Оболочки операционных систем.	
	Работа в консольном и графическом режимах	
<b>Тема 1.4.</b> Управление памятью	<b>Содержание</b>	
	ТЗ.7 Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. К.1 Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти	2 2
	ПЗ.5 Мониторинг за использованием памяти	2
<b>Тема 1.5.</b> Управление процессами, многопроцессорные системы	<b>Содержание</b>	
	ПЗ.6 Понятие процесса. Понятие потока.	2
	ПЗ.7 Понятие приоритета и очереди процессов, особенности многопроцессорных систем.	2
	СР.1 Межпроцессорное взаимодействие	2
	Понятие взаимоблокировки. ПЗ.8 Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок.	2
	Предотвращение взаимоблокировок	
	СР.2 Управление процессами	2
Наблюдение за использованием ресурсов системы		
<b>Тема 1.6.</b> Виртуализация и облачные технологии	<b>Содержание</b>	
	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода.	2
	ПЗ.9 Виртуальные устройства. Вопросы лицензирования	
	К.2 Облачные технологии. Исследования в области виртуализации и облаков	2
	ПЗ.10 Изучение примеров виртуальных машин (VMware, VBox)	2
	<b>Контрольная работа (промежуточная аттестация)</b>	
	<b>Итого за семестр</b>	42 ч
<b>Раздел 2. Безопасность операционных систем</b>		
	<b>Содержание</b>	

<b>Тема 2.1.</b> Принципы построения защиты информации в операционных	ТЗ.8 Понятие безопасности ОС. Классификация угроз ОС.	2
	ПЗ.11 Источники угроз информационной безопасности и объекты воздействия.	2
	ТЗ.9 Порядок обеспечения безопасности информации при эксплуатации операционных систем.	2
	ТЗ.10 Штатные средства ОС для защиты информации.	2

системах	ТЗ.11 Аутентификация, авторизация, аудит.	2
	ПЗ.12 Управление учетными записями пользователей и доступом к ресурсам	2
	К.3 Аудит безопасности организации	2
	ПЗ.13 Аудит событий системы	2
	СР.3 Анализ журнала аудита ОС на рабочем месте	2
	ПЗ.14 Изучение штатных средств защиты информации в операционных системах СР.4 Изучение штатных средств защиты информации в операционных системах	2
<b>Раздел 3. Особенности работы в современных операционных системах</b>		
<b>Тема 3.1.</b> Операционные системы UNIX, Linux, MacOS и Android	<b>Содержание</b>	
	ТЗ.12 Обзор системы Linux. Процессы в системе Linux.	2
	ПЗ.15 Управление памятью в Linux.	2
	ПЗ.16 Ввод-вывод в системе Linux.	2
	ПЗ.17 Файловая система UNIX.	2
	ПЗ.18 Создание дистрибутива Linux. Установка.	2
	ТЗ.13 Операционные системы семейства Mac OS: особенности, преимущества и недостатки.	2
	ПЗ.19 Архитектура Android. Приложения Android	2
ПЗ.19 Работа в ОС Linux.	2	
<b>Тема 3.2.</b> Операционная система Windows	<b>Содержание</b>	<b>2</b>
	ТЗ.15 Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	
	ПЗ.20 Установка и первичная настройка Windows.	
<b>Тема 3.3.</b> Серверные операционные системы	<b>Содержание</b>	<b>2</b>
	ТЗ.16 Назначение и особенности серверных ОС.	
	ПЗ.21 Распределенные файловые системы.	
	<b>ПЗ.22</b> Установка Windows Server 16. Active Directory.	<b>4</b>
	<b>ПЗ.23</b> Установка и настройка ALT Linux	
	<b>К.4</b> Изучение аналитических обзоров в области построения систем безопасности ОС.	
	СР.5 Работа с сетевой файловой системой.	
К.5 Работа с серверной ОС, например, AltLinux.		
Итого за семестр		<b>54</b>

<b>Производственная практика по ПП 01.01</b>	<b>36</b>
<b>Итого по РАЗДЕЛУ 1</b>	<b>132</b>

<b>РАЗДЕЛ 2</b>		
<b>МДК.01.02 Базы данных</b>		<b>162</b>
<b>Раздел 1. Основы теории баз данных</b>		
<b>Тема 1.1.</b> Основные понятия теории баз данных. Модели данных	<b>Содержание</b>	
	ТЗ.1 Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. ТЗ.2 Объекты, свойства, отношения. Централизованное управление данными, основные требования.	2 2
	К.1 Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных.	2
	Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	
<b>Тема 1.2.</b> Основы реляционной алгебры	<b>Содержание</b>	
	ТЗ.3 Основы реляционной алгебры.	2
	ПЗ.1 Традиционные операции над отношениями.	2
	ПЗ.2 Специальные операции над отношениями.	2
	ПЗ.3 Операции над отношениями. Выборка, объединение, пересечение, разность	2
ПЗ.4 Операции над отношениями. Декартова произведения и соединения	2	
<b>Тема 1.2.</b> Базовые понятия и классификация систем управления базами данных	<b>Содержание</b>	
	ТЗ.4 Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД.	2
	ТЗ.5 Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору)	2
	ПЗ.5 Семиуровневая модель OSI.	
	ПЗ.6 Взаимодействие между уровнями модели OSI.	
	ПЗ.7 Математическое представление сигналов связи.	
	ПЗ.8 Графическое представление сигналов связи.	
	ПЗ.9 Математическое и графическое представление сигналов связи.	
	ПЗ.10 Изучение элементов кабельной системы.	

	СР.1 Тенденции развития БД СР.2 Развитие СУБД	
<b>Тема 1.3.</b> Целостность данных как ключевое понятие баз данных	<b>Содержание</b> ТЗ.6 Понятие целостности и непротиворечивости данных. ПЗ.11 Примеры нарушения целостности и непротиворечивости данных. К.2 Правила и ограничения. Контрольная работа.	 2 2 2
	<b>Итого за семестр</b>	<b>42</b>
<b>Раздел 2. Проектирование баз данных</b>		
<b>Тема 2.1.</b>	<b>Содержание</b>	<b>2</b>

Информационные модели реляционных баз данных	ТЗ.3 Типы информационных моделей. Логические модели данных. Физические модели данных.	2
	ПЗ.12 Проектирование логической модели данных	2
	ПЗ.13 Проектирование физической модели данных	2
	СР.3 Проектирование инфологической модели данных	2
<b>Тема 2.2.</b> Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	<b>Содержание</b>	
	ТЗ.8 Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам.	2
	ТЗ.9 Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.	2
	ПЗ.14 Методика проектирования базы данных	2
<b>Тема 2.3.</b> Средства автоматизации проектирования	ПЗ.15 Проектирование базы данных	2
	ТЗ.10 CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств.	2
	ТЗ.11 Графическое представление моделей проектирования.	2
	ТЗ.12 UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	2
	ПЗ.16 Проектирование базы данных с использованием CASE-средств	2
	ПЗ.17 Разработка и сопровождение баз данных с использованием CASE-средств	2
<b>Раздел 3. Организация баз данных</b>		
<b>Тема 3.1.</b> Создание базы данных. Манипулирование данными.	ТЗ.13 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.	2
	ТЗ.14 Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.	2
	<b>ПЗ.18</b> Создание базы данных средствами СУБД.	2
	ПЗ.19 Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	2
	СР.4 Создание пользовательского приложения средствами СУБД	2
<b>Тема 3.2.</b> Индексы. Связи между таблицами.	<b>ТЗ.15</b> Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы.	2
	ПЗ.20 Связи между таблицами реляционной базы данных.	2

	К.3 Создание взаимосвязей	2
	ПЗ.21 Сортировка, поиск и фильтрация данных	2
<b>Раздел 4. Управление базой данных с помощью SQL</b>		
<b>Тема 4.1.</b> Структурированный язык запросов SQL	<b>ТЗ.16</b> Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL	<b>2</b>
	ТЗ.17 Команды определения данных и манипулирования данными.	2
	<b>ПЗ.22</b> Создание базы данных с помощью команд SQL	<b>2</b>
	<b>ПЗ.23</b> Редактирование, вставка и удаление данных средствами языка SQL	2
<b>Тема 4.2.</b> Операторы и функции языка SQL		<b>2</b>
	ТЗ.18 Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	
	<b>Тематика практических занятий</b>	
	ПЗ.24 Создание и использование запросов. Группировка и агрегирование данных	2
	ПЗ.25 Создание в запросах вычисляемых полей.	2
	ПЗ.26 Использование условий	2
<b>Раздел 5. Организация распределённых баз данных</b>		
<b>Тема 5.1.</b> Архитектуры распределённых баз данных	ТЗ.19 Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД	<b>2</b>
	ПЗ.27 Управление доступом к объектам базы данных	<b>2</b>
	ПЗ.28 Управление доступом в СУБД MySQL	<b>2</b>
<b>Тема 5.2.</b> Серверная	<b>Содержание</b>	

часть распределенной базы данных	ТЗ.20 Планирование и развёртывание СУБД для работы с клиентскими приложениями	2	
	ПЗ.29 Установка СУБД. Настройка компонентов СУБД.	2	
<b>Раздел 6. Администрирование и безопасность</b>			
<b>Тема 6.1.</b> Обеспечение целостности, достоверности и непротиворечивости данных.	<b>Содержание</b>	<b>2</b>	
	ТЗ.21 Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения.		<b>2</b>
	ТЗ.22 Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера.		<b>2</b>
	К.4 Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.		<b>2</b>
	ПЗ.30 Разработка хранимых процедур		<b>2</b>
	ПЗ.31 Разработка триггеров	2	
<b>Тема 6.3. Механизмы</b>	<b>Содержание</b>		

защиты информации в системах управления базами данных	ТЗ.23 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	2
	ПЗ.32 Управление правами доступа к базам данных	<b>2</b>
	ПЗ.33 Разбор синтаксиса хранимых процедур	2
	ПЗ.34 Разбор синтаксиса триггеров	2
	К.5 Разбор синтаксиса хранимых процедур и триггеров	2
СР.5 Контрольная работа	2	
	Итого за семестр	90
<b>Производственная практика ПП 01.02</b>		36
<b>ВСЕГО ПО РАЗДЕЛУ 2</b>		<b>162</b>

<b>РАЗДЕЛ 3</b>		<b>78</b>
<b>МДК.01.03 Сети и системы передачи информации</b>		<b>42</b>
<b>Раздел 1. Теория телекоммуникационных сетей</b>		
<b>Тема 1.1.</b> Основные понятия и определения	ТЗ.1 Основы передачи сигналов в системах связи.	<b>2</b>
	ТЗ.2 Основы организации сетей и принципы многоуровневого взаимодействия	<b>2</b>
<b>Тема 1.2.</b> Принципы передачи информации в сетях и системах связи	<b>Содержание</b>	
	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	
<b>Тема 1.3.</b> Типовые каналы передачи и их характеристики	<b>Содержание</b>	
	ТЗ.3 Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	<b>2</b>

	ПЗ.1 Расчет пропускной способности канала связи	2
	ПЗ.2 Расчет пропускной способности канала связи	2
<b>Раздел 2. Сети передачи данных</b>		
<b>Тема 2.1.</b> Архитектура и принципы работы современных сетей передачи данных	<b>Содержание</b>	
	Структура и характеристики сетей.	
	ТЗ.4 Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи.	2
	К.1 Изучение сетевых утилит	2
	ТЗ.5 Протоколы и интерфейсы управления каналами и сетью передачи данных.	2
	ПЗ.3 Конфигурирование сетевого интерфейса рабочей станции	2
	ПЗ.4 Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP	2
	СР.1 Конфигурирование сетевого интерфейса	2
	ПЗ.5 Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне	2
	ПЗ.6 Диагностика и разрешение проблем сетевого уровня	2
ПЗ.7 Диагностика и разрешение проблем протоколов транспортного уровня	2	
ПЗ.8 Диагностика и разрешение проблем протоколов прикладного уровня	2	
<b>Тема 2.2.</b> Беспроводные системы передачи данных	<b>Содержание</b>	
	ТЗ.6 Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	2
	ПЗ.9 Настройка Wi-Fi маршрутизатора	2
	ПЗ.10 Настройка Wi-Fi маршрутизатора	2
	К.2 Настройка Wi-Fi маршрутизатора	2
	СР.2 Маршрутизация и управление потоками в сетях связи	2
	ТЗ.7 Принципы функционирования систем сотовой связи	2
<b>Производственная практика ПП 01.03</b>		36
<b>ВСЕГО ПО РАЗДЕЛУ 3</b>		<b>78</b>

<b>РАЗДЕЛ 4</b>		<b>218</b>
<b>МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении</b>		
<b>Раздел 1. Разработка защищенных автоматизированных (информационных) систем</b>		
<b>Тема 1.1. Основы информационных систем как объекта защиты.</b>	<b>Содержание</b>	
	ТЗ.1 Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС.	2
	ТЗ.2 Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.	2
	Основные особенности современных проектов АИС. ТЗ.3 Электронный документооборот.	2
	ПЗ.1 Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	2
<b>Тема 1.2. Жизненный цикл автоматизированных систем</b>	ПЗ.2 Автоматизированная информационная система компании	2
	ТЗ.4 Жизненный цикл АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.	2
	ТЗ.5 Проектирование АИС Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.	2
	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.	
	ПЗ.3 Разработка технического задания на проектирование автоматизированной системы	2
	ПЗ.4 Разработка технического задания на проектирование АИС	2
<b>Тема 1.3. Угрозы безопасности информации в автоматизированных</b>	К.1 Разработка концепции защиты автоматизированной (информационной) системы.	<b>2</b>
	ТЗ.6 Классификация угроз безопасности АИС. Банк данных угроз безопасности. Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк	2

	данных угроз безопасности информации СР.1 Анализ угроз безопасности информации	2
--	---	---

системах	ТЗ.7 Понятие уязвимости угрозы. Классификация уязвимостей.	
	<b>ПЗ.5</b> Категорирование информационных ресурсов	2
	ПЗ.6 Категорирование информационных ресурсов	2
	ПЗ.7 Анализ угроз безопасности информации	2
	ПЗ.8 Анализ угроз безопасности информации	2
	ПЗ.9 Построение модели угроз	2
<b>Тема 1.4.</b> Основные меры защиты информации в автоматизированных системах	ТЗ.8 Обзор мер защиты информации в автоматизированных системах	2
	СР.2 Построение сводной матрицы угроз автоматизированной (информационной) системы	2
	ТЗ.9 Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	2
<b>Тема 1.5.</b> Содержание и порядок эксплуатации АС в защищенном исполнении	<b>Содержание</b>	
	ТЗ.10 Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	
	Ограничение программной среды. ТЗ.11 Защита машинных носителей информации	
	Регистрация событий безопасности	
	ТЗ.12 Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	
	ТЗ.13 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.	
	ТЗ.14 Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных	
	Резервное копирование и восстановление данных.	

	Сопровождение автоматизированных систем. К.2 Управление рисками и инцидентами управления безопасностью.	
<b>Тема 1.6.</b> Защита информации в распределенных автоматизированных системах	<b>Содержание</b>	
	ТЗ.15 Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем.	2
	Экзамен по МДК 01.04	18
	<b>Итого за семестр</b>	<b>74</b>
	ТЗ.16 Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	2
<b>Тема 1.7.</b> Особенности разработки информационных систем персональных данных	<b>ТЗ.17</b> Общие требования по защите персональных данных.	<b>2</b>
	Состав и содержание организационных и технических мер по защите информационных систем персональных данных. ТЗ.18 Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	2
	ПЗ.10 Определения уровня защищенности ИСПДн	2
	ПЗ.11 Выбор мер по обеспечению безопасности ПДн. ПЗ.12 Категорирование информационных ресурсов	2 2
<b>Раздел 2. Эксплуатация защищенных автоматизированных систем.</b>		
<b>Тема 2.1.</b> Особенности эксплуатации автоматизированных систем в защищенном исполнении.	<b>Содержание</b>	
	ТЗ.19 Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	2
	ТЗ.20 Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	2
	СР.3 Анализ журнала аудита на рабочем месте	2
	К.3 Проведение внутреннего аудита АИС	2

	ТЗ.21 Выявление угроз информационной безопасности автоматизированных систем.	2
	ТЗ.22 Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	2
<b>Тема 2.2.</b>	<b>ТЗ.23</b> Задачи и функции администрирования автоматизированных систем.	<b>2</b>
Администрирование автоматизированных систем	Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. ТЗ.24 Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	2

<b>Тема 2.3.</b> Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	<b>ТЗ.25</b> Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.	<b>2</b>
	ТЗ.26 Общие обязанности администратора информационной безопасности автоматизированных систем.	2
<b>Тема 2.4.</b> Защита от несанкционированного доступа к информации	<b>К.4</b> Основные принципы защиты от НСД.	<b>2</b>
	ТЗ. 27 Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.	2
	Классификация автоматизированных систем. ТЗ.28 Требования по защите информации от НСД для АС	2
	ТЗ.29 Требования защищенности СВТ от НСД к информации	2
	ТЗ.30 Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	2
<b>Тема 2.5.</b> СЗИ от НСД	Назначение и основные возможности системы защиты от несанкционированного доступа. <b>ТЗ.31</b> Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.	2
	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	

	ПЗ.13 Установка и настройка СЗИ от НСД	2
	СР.4 Методы применения СЗИ от НСД	2
	К.5 Анализ политик безопасности информационного объекта	2
	ТЗ.32 Управление доступом. Разграничение доступа	2
	ПЗ.14 Защита входа в систему (идентификация и аутентификация пользователей)	2
	ПЗ.15 Разграничение доступа к устройствам	2
	ТЗ.33 Правила работы с конфиденциальными ресурсами.	2
	ПЗ.16 Управление доступом	2
	ПЗ.17 Использование принтеров для печати конфиденциальных документов. Контроль печати	2
	СР.5 Методы контроля печати конфиденциальных документов	2
	ТЗ.34 Обеспечение целостности информационной системы	2
	ТЗ.35 Централизованное управление системой защиты.	2
	ПЗ.18 Настройка системы для задач аудита	2
	ПЗ.19 Настройка контроля целостности и замкнутой программной среды	2
	ПЗ.20 Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	2
	СР.6 Оперативный мониторинг и аудит безопасности	2
<b>Тема 2.6.</b> Эксплуатация средств защиты информации в компьютерных сетях	<b>Содержание</b>	
	ТЗ.36 Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	2
	ТЗ.37 Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	2
	ТЗ.38 Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов. К.6 Восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	2
	ТЗ.39 Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	2
	ПЗ.21 Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	2
	ПЗ.22 Настройка и устранение неисправности программно-аппаратных СЗИ	2

<b>Тема 2.7.</b> Документация на защищаемую автоматизированную систему	ТЗ.40 Основные эксплуатационные документы защищенных автоматизированных систем.	<b>2</b>
	ПЗ.23 Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	2
	ПЗ.24 Оформление основных эксплуатационных документов на автоматизированную систему.	2
	СР.7 Анализ ПО в области определения рисков ИБ информации	2
	К.7 Консультация	2
	<b>Итого за семестр</b>	<b>90</b>
<b>Производственная практика ПП 01.04</b>		54
<b>ВСЕГО ПО РАЗДЕЛУ 4</b>		<b>218</b>

<b>РАЗДЕЛ 5</b>		<b>164</b>
<b>МДК.01.05. Эксплуатация компьютерных сетей</b>		
<b>Раздел 1. Основы передачи данных в компьютерных сетях</b>		
<b>Тема 1.1.</b> Модели сетевого взаимодействия	<b>Содержание</b>	<b>2</b>
	Модель OSI. ТЗ.1 Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.	
	Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP. ПЗ.1 Изучение элементов кабельной системы.	<b>2</b>
<b>Тема 1.2.</b> Физический уровень модели OSI	<b>Содержание</b>	<b>2</b>
	ТЗ.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	<b>2</b>
	ТЗ.3 Стандарты кабелей. Электрическая проводка.	
	Беспроводная среда передачи.	
ПЗ.2 Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	<b>2</b>	
Сварка оптического волокна		

<b>Тема 1.3.</b> Топология компьютерных сетей	<b>Содержание</b>	<b>2</b>
	ТЗ.4 Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.	
	ПЗ.3 Разработка топологии сети небольшого предприятия	2
	ПЗ.4 Построение одноранговой сети	2
<b>Тема 1.4.</b> Технологии Ethernet	<b>Содержание</b>	<b>2</b>
	ТЗ.5 Обзор технологий построения локальных сетей. Технология Ethernet. Физический уровень. Технология Ethernet. Канальный уровень	
	ПЗ.5 Изучение адресации канального уровня. MAC-адреса.	2
<b>Тема 1.5.</b> Технологии коммутации	<b>Содержание</b>	<b>2</b>
	ТЗ.6 Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	
	К.1 Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети	
	Технология PoweroverEthernet	<b>2</b>
	ПЗ.6 Создание коммутируемой сети	
<b>Тема 1.6.</b> Сетевой протокол IPv4	<b>Содержание</b>	<b>2</b>
	ТЗ.7 Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов. Маршрутизация пакетов IPv4 Протоколы динамической маршрутизации	
	ПЗ.7 Изучение IP-адресации.	2
<b>Тема 1.7.</b> Скоростные	<b>Содержание</b>	

и беспроводные сети	Сеть FDDI. Сеть 100VG-AnyLAN СР.1 Сверхвысокоскоростные сети Беспроводные сети	2
	ПЗ.8 Настройка беспроводного сетевого оборудования	2
<b>Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet</b>		
<b>Тема 2.1.</b> Основы коммутации	<b>Содержание</b>	2
	Функционирование коммутаторов локальной сети. ТЗ.8 Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах.	
	Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов	
	ПЗ.9 Работа с основными командами коммутатора.	2
<b>Тема 2.2.</b> Начальная настройка коммутатора	<b>Содержание</b>	2
	СР.2 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.	
	ПЗ.10 Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	2
	ПЗ.11 Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	2
<b>Тема 2.3.</b> Виртуальные локальные сети (VLAN)	<b>Содержание</b>	2
	К.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	

	ПЗ.12 Настройка VLAN на основе стандарта IEEE 802.1Q	2
	ПЗ.13 Настройка протокола GVRP.	2
	ПЗ.14 Настройка сегментации трафика без использования VLAN	2
	ПЗ.15 Настройка функции Q-in-Q (Double VLAN).	2
	ПЗ.16 Настройка протоколов связующего дерева STP, RSTP, MSTP.	2
	Промежуточная аттестация	18
	<b>Итого за семестр</b>	<b>74</b>
<b>Тема 2.4.</b> Функции повышения надежности и производительности	<b>Содержание</b>	
	Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.	
	Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.	
	Дополнительные функции защиты от петель. Агрегирование каналов связи.	
	Настройка протоколов связующего дерева STP, RSTP, MSTP.	
	ПЗ.17 Настройка функции защиты от образования петель LoopBackDetection	2
	ПЗ.18 Агрегирование каналов.	2
<b>Тема 2.5.</b> Адресация сетевого уровня и маршрутизация	<b>Содержание</b>	
	ТЗ.9 Обзор адресации сетевого уровня. Формирование подсетей.	2
	ТЗ.10 Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.	2
	Протокол IPv6. Формирование идентификатора интерфейса.	
	ПЗ.19 Способы конфигурации IPv6-адреса.	2
	ПЗ.20 Планирование подсетей IPv6. Протокол NDP. Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.	2
	Основные конфигурации маршрутизатора.	
	Расширенные конфигурации маршрутизатора.	
	ПЗ.21 Работа с протоколом CDP. Работа с протоколом TELNET. Работа с протоколом TFTP.	2
ПЗ.22 Работа с протоколом RIP. Работа с протоколом OSPF.	2	

	ПЗ.23 Конфигурирование функции маршрутизатора NAT/PAT.	2
	СР.3 Конфигурирование PPP и CHAP.	2
	К.3 Создание структуры сети организации	2
<b>Тема 2.6.</b> Качество обслуживания (QoS)	<b>Содержание</b>	
	ТЗ.11 Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	2
	ТЗ.12 Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.	2
	ПЗ.24 Настройка QoS. Приоритизация трафика.	2
	ПЗ.25 Управление полосой пропускания	2
<b>Тема 2.7.</b> Функции обеспечения безопасности и ограничения доступа к сети	<b>Содержание</b>	
	ТЗ.13 Списки управления доступом (ACL). ТЗ.14 Функции контроля над подключением узлов к портам коммутатора.	2 2
	Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.	
	ПЗ.26 Списки управления доступом (AccessControlList)	2
	ПЗ.27 Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.	2
	Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	
<b>Тема 2.8.</b> Многоадресная рассылка	<b>Содержание</b>	
	ТЗ.15 Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.	2
	Подписка и обслуживание групп. ПЗ.28 Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping). Функция IGMP FastLeave.	2
	СР.4 Определение уязвимых мест сети	2
	К.4 Определение требований к обеспечению безопасности сети	2
	ПЗ.29 Функция IGMP FastLeave.	2
	ПЗ.30 Отслеживание трафика многоадресной рассылки.	2
	ПЗ.31 Отслеживание трафика Multicast	2
<b>Тема 2.9.</b> Функции управления коммутаторами	<b>Содержание</b>	
	ТЗ.16 Управление множеством коммутаторов. Протокол SNMP.	
	ПЗ.32 RMON (Remote Monitoring). Функция Port Mirroring.	2 2
	ПЗ.33 Функции анализа сетевого трафика.	2

	ПЗ.34 Настройка протокола управления топологией сети LLDP.	2
<b>Раздел 3. Межсетевые экраны</b>		
<b>Тема 3.1.</b> Основные принципы создания надежной и безопасной ИТ-инфраструктуры	<b>Содержание</b>	
	ТЗ.17 Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.	2
	ТЗ.18 Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.	2
<b>Тема 3.2.</b> Межсетевые экраны	<b>Содержание</b>	
	ТЗ.19 Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.	2
	ТЗ.20 Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.	2
	<b>ТЗ.21</b> Планирование и внедрение межсетевого экрана.	2
	ПЗ.35 Основы администрирования межсетевого экрана	2
	ПЗ.36 Соединение двух локальных сетей межсетевыми экранами	2
	ПЗ.37 Создание политики без проверки состояния.	2
	Создание политик для традиционного (или исходящего) NAT.	
	Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing	
<b>Тема 3.3.</b> Системы обнаружения и предотвращения проникновений	<b>Содержание</b>	
	ТЗ.22 Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.	2
	ПЗ.38 Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.	2
	ПЗ.39 Обнаружение и предотвращение вторжений.	2
<b>Тема 3.4.</b> Приоритизация трафика и создание альтернативных маршрутов	<b>Содержание</b>	
	ТЗ.23 Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.	2
	ПЗ.40 Создание альтернативных маршрутов с использованием статической маршрутизации	2

	СР.5 Проектирование виртуальных частных сетей	2
	К.5 Проектирование виртуальных частных сетей	2
	<b>Производственная практика ПП 01.05</b>	<b>54</b>
	<b>Итого по разделу 5</b>	<b>164</b>
	<b>Экзамен по профессиональному модулю</b>	<b>18</b>
	<b>ВСЕГО ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ</b>	<b>832</b>

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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

лаборатория Информационных технологий, программирования и баз данных; лаборатория Сетей и систем передачи информации, лаборатория Программных и программно-аппаратных средств защиты информации, оснащенные в соответствии с ОПОП по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики, в соответствии с ОПОП по данной специальности.

**3.1.1. Требования к материально-техническому обеспечению обучающихся с РАС**

В учебных аудиториях (по возможности) стараться избегать использования ламп дневного света с дросселями, т.к. они мерцают и издают гул. Преимущественное использование светодиодов или ламп дневного света с качественным электронным балластом.

В аудиториях не должно быть гула или стробоскопического эффекта. Обеспечение хорошей акустики: не должно быть эха, посторонних шумов и т.п.

**3.2. Реализация адаптированной программы профессионального модуля предполагает обязательную учебную и производственную практики.**

Требования к оснащению баз практик в соответствии с п. 6.3.7 АОП СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

**Требования к организации практической подготовки обучающихся с инвалидностью и/или ограниченными возможностями здоровья (РАС)**

Для обучающихся с РАС проведение практической подготовки устанавливается образовательной организацией с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья. При определении мест прохождения учебной и производственных практик, обучающихся с РАС образовательная организация должна учитывать рекомендации, данные по результатам медико-социальной экспертизы, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда. (например, при непреодолимых препятствиях: непереносимости запахов в лаборатории, шумов в цехах и т.п.)

**3.3. Информационное обеспечение реализации адаптированной программы**

**3.3.1** Для реализации адаптированной программы библиотечный фонд колледжа имеет печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе.

При формировании библиотечного фонда выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

Обучающиеся инвалиды и лица с ограниченными возможностями здоровья обеспечены печатными и (или) электронными учебными изданиями, адаптированными при необходимости для обучения указанных обучающихся.

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется настоящей адаптированной рабочей программой и подлежит обновлению (при необходимости).

**3.3.2. Учебно-методическое обеспечение реализации адаптированной программы обучающихся с РАС**

Предоставление презентаций, конспектов, видеозаписей занятий и т.п. Структурировано оформленные фонды оценочных средств. Дополнительные подробные инструкции и пояснения для выполнения задания.

### 3.3.3 Основные печатные источники

1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2024. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2024.
2. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2024.
3. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2023.
4. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2024.
5. Сеницын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2023.
6. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2026.
7. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2023.

### 3.3.2. Дополнительные печатные источники:

1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2022.
2. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2022. – 224 с.
3. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб.: Питер, 2023 - 703 с.
4. Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2022. - 88 с.
5. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бинوم, 2021. – 1024 с.
6. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бинوم, 2021. – 704 с.
7. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2021
8. Кофлер М., Linux. Полное руководство – Питер, 2021. – 800 с.
9. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2021
10. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2021.- 531 с.
11. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2021. – 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, 2021.- 147 с.
13. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2023. – 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, 2021. – 240 с.

15. Руссинович М., Соломон Д., Внутреннее устройство MicrosoftWindows. Основные подсистемы операционной системы – Питер, 2024. – 672 с.

16. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2021. – 368 с.

### **3.3.3. 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/>

### **3.3.4. Электронные источники:**

1. Информационно-справочная система по документам в области технической защиты информации [www.fstec.ru](http://www.fstec.ru)

2. Информационный портал по безопасности [www.SecurityLab.ru](http://www.SecurityLab.ru).

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

4. Российский биометрический портал [www.biometrics.ru](http://www.biometrics.ru)

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

6. Сайт Научной электронной библиотеки [www.elibrary.ru](http://www.elibrary.ru)

7. Справочно-правовая система «Гарант» » [www.garant.ru](http://www.garant.ru)

8. Справочно-правовая система «Консультант Плюс» [www.consultant.ru](http://www.consultant.ru)

9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru)

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

11. Федеральный портал «Российское образование [www.edu.ru](http://www.edu.ru)

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

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

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

Для осуществления процедур текущего контроля успеваемости, промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для обучающихся инвалидов и лиц с ограниченными возможностями здоровья, позволяющие оценить достижение ими результатов обучения и уровень сформированности всех компетенций, предусмотренных адаптированной образовательной программой.

Форма проведения текущей аттестации для обучающихся с ограниченными возможностями здоровья и инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа при прохождении аттестации.