

Министерство образования Ставропольского края
Государственное бюджетное профессиональное образовательное учреждение
«Пятигорский техникум торговли, технологий и сервиса»
(ГБПОУ ПТТТиС)

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация – техник по защите информации

2024 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	12
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	15
4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	50

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

1.1. Область применения программы.

Рабочая программа профессионального модуля (далее рабочая программа) – является частью основной профессиональной образовательной программы по специальности СПО в соответствии с ФГОС по специальности СПО образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» укрупненной группы 10.00.00 Информационная безопасность базовой подготовки в части освоения основного вида профессиональной деятельности (ВПД):

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении соответствующих профессиональных компетенций (ПК):

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

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

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

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

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

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

1.3. В результате освоения профессионального модуля должен:

Иметь практический опыт:	установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; администрирования автоматизированных систем в защищенном исполнении; эксплуатации компонентов систем защиты информации автоматизированных
---------------------------------	--

	<p>систем;</p> <p>диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении</p> <p>Настройки программно-аппаратных средств защиты информации, в том числе антивирусной защиты в операционных системах по заданным шаблонам;</p> <p>Инструктажа пользователей по порядку работы в операционных системах;</p> <p>Оформления эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах;</p> <p>Ввода в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях;</p> <p>Установки средств межсетевого экранирования в соответствии с действующими требованиями по защите информации</p> <p>Инструктажа пользователей по порядку безопасной работы в компьютерных сетях;</p> <p>Оформления эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях;</p> <p>Определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях.</p>
<p>уметь:</p>	<p>осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;</p> <p>организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;</p> <p>осуществлять конфигурирование,</p>

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

Выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных

Выполнять настройку параметров работы программного обеспечения, средства электронного документооборота

Работать с программным обеспечением с соблюдением действующих требований по защите информации

Контролировать процесс управления учетными записями пользователей СУБД

Контролировать неизменность настроек средств защиты информации

Работать в компьютерных сетях с соблюдением действующих требований по защите информации. Конфигурация и контроль корректности настройки программно-аппаратных средств защиты информации в компьютерных сетях

Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях.

Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях

Разрабатывать техническое задание на создание подсистем информационной безопасности автоматизированных систем

Исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью

обеспечения требуемого уровня защищенности

Работать с программным обеспечением с соблюдением действующих требований по защите информации

Определять элементы кабельной системы, защищенные от НСД

Определять оптимальность выбора аппаратных средств защиты информации

Оценивать режимы выбора аппаратных средств защиты информации функционирования в компьютерных сетях

Применять программно-аппаратных средств защиты информации в компьютерных сетях

Настраивать правила фильтрации пакетов в компьютерных сетях

Определять правила фильтрации пакетов в компьютерных сетях

Настраивать правила фильтрации пакетов в компьютерных сетях с применением IPv4

Оценивать оптимальности выбора аппаратных средств защиты информации

Настраивать правила фильтрации пакетов и преобразование сетевых адресов

Настраивать правила фильтрации пакетов с использованием NAT

Настраивать правила фильтрации пакетов с использованием скрытого NAT

Определять предложения по применению программных средств защиты информации в компьютерных сетях

Определять предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях

Настраивать правила SpanningTreeProtocol в компьютерных сетях

Определять правильность выбора аппаратно-программных средств защиты

Вносить предложения по применению средств защиты информации в режиме функционирования

Настраивать правила фильтрации пакетов в модели QoS

	<p>Управлять количеством подключаемых к портам коммутатора пользователей</p> <p>Работать со снифферами</p> <p>Работать со стандартом IEEE 802.1AB-2009</p> <p>Фильтровать трафик между сетями или узлами сети</p> <p>Фильтровать трафик на основе MAC-адресов</p> <p>Работать с персональными межсетевыми экранами</p> <p>Работать с правилами фильтрации с использованием NAT</p> <p>Настраивать Сетевую Систему обнаружения вторжений</p> <p>Настраивать Сетевую Систему обнаружения вторжений, основанной на прикладных протоколах APIDS</p> <p>Блокировать атаки с помощью межсетевого экрана</p> <p>Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях</p>
<p>знать:</p>	<p>состав и принципы работы автоматизированных систем, операционных систем и сред;</p> <p>принципы разработки алгоритмов программ, основных приемов программирования;</p> <p>модели баз данных;</p> <p>принципы построения, физические основы работы периферийных устройств;</p> <p>теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;</p> <p>порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;</p> <p>принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.</p>

Порядок обеспечения безопасности информации при эксплуатации операционных систем

Типовые средства защиты информации в операционных системах

Встроенный в Microsoft Windows межсетевой экран Брандмауэр Windows

Сканер системы Windows Defender

Планирование систем и их приемка

Шифрование съемных носителей информации

Использование правила политики безопасности «Deny write access to removable drives not protected BitLocker»

Виды политик управления доступом и информационными потоками применительно к операционным системам

Формы инструктажа пользователей по порядку работы в операционных системах

Методы инструктажа пользователей по порядку работы в операционных системах

Порядок настройки программного обеспечения систем управления базами данных и средств электронного документооборота

Методы установки ПО рабочих станций и сервера

Проверка работоспособности системы

Восстановление работоспособности системы

Оптимизация работоспособности системы

Настройка работоспособности системы управления базами данных.

Состав типовых конфигураций коммутаторов для обеспечения безопасного функционирования

Типовые конфигурации программно-аппаратных средств защиты информации

Режимы функционирования программно-аппаратных средств защиты информации в компьютерных сетях

Порядок реализации методов межсетевого экранирования

Управляемые коммутаторы

	Порядок реализации программных средств межсетевого экранирования Порядок реализации программно-аппаратных средств межсетевого экранирования Организация эффективной работы средств межсетевого экранирования Виды политик управления доступом в компьютерных сетях Виды политик управления информационными потоками в компьютерных сетях Пассивные и активные системы обнаружения вторжений Альтернативные таблицы маршрутизации. Правила выбора таблиц. Ограничение (шейпинг) трафика
--	---

1.4. Количество часов на освоение программы профессионального модуля:

Всего часов -- 760 часов

В том числе в форме практической подготовки – 366 часов

Из них на освоение МДК 01.01 -- 98 часов

В том числе самостоятельная работа – 2 часа

Промежуточная аттестация в форме экзамена

Из них на освоение МДК 01.02 --98 часов

В том числе самостоятельная работа – 2 часа

Промежуточная аттестация в форме экзамена

Из них на освоение МДК 01.03 --68 часа

В том числе самостоятельная работа – 2 часа

Промежуточная аттестация в форме дифференцированного зачета

Из них на освоение МДК 01.04 --120 часов

В том числе самостоятельная работа – 2 часа

Промежуточная аттестация в форме экзамена

Из них на освоение МДК 01.05 --196 часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

2.1.1 Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) Эксплуатация автоматизируемых (информационных) систем в защищенном исполнении, в том числе профессиональными (ПК), общими (ОК) компетенциями и личностными результатами (ЛР).

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.

2.1.2. Перечень профессиональных компетенций

Код	Наименование результата обучения
-----	----------------------------------

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.
ПК1. 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.

2.1.3. Перечень личностных результатов:

ЛР 1.	Осознающий себя гражданином и защитником великой страны
ЛР 2.	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 3.	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР 4.	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде лично и профессионального конструктивного «цифрового следа»
ЛР 5.	Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России

ЛР.6	Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях
ЛР.7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
ЛР.8	Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства
ЛР.9.	Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях
ЛР 10.	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛР 11.	Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры
ЛР 12.	Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания
ЛР КК 1.	Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы, управляющий собственным профессиональным развитием, рефлексивно оценивающий собственный жизненный опыт, критерии успешности
ЛР КК 2.	Экономически активный, предприимчивый, готовый к самозанятости

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля

Коды профессиональных и общих компетенций, личностных результатов	Наименования разделов профессионального модуля	Объем профессионального модуля, ак.час.							Самостоятельная работа
		Всего, ч	В т.ч. в форме практ. подготовки	Работа обучающихся во взаимодействии с преподавателем					
				Обучение по МДК			Практики		
				Всего	В том числе		Учебная	Производственная	
Лаборат. и практ. занятий	Курсовых работ (проектов)								
1	2	3	4	5	6	7	8	9	10
ПК 1.1 ОК 1-10 ЛР 1-11, КК1, КК2	МДК 01.01 Операционные системы	98	36	78	36	-	18	-	2
ПК 1.1 ОК 1-10 ЛР 1-11, КК1, КК2	МДК 01.02 Базы данных	98	40	78	40	-	18	-	2
ПК 1.2-ПК 1.4 ОК 1-10 ЛР 1-11, КК1, КК2	МДК.01.03 Сети и системы передачи информации	68	20	42	20	--	24	-	2
ПК 1.2-ПК 1.4 ОК 1-10 ЛР 1-11, КК1, КК2	МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	120	30	94	30	-	24	-	2
ПК 1.2-ПК 1.4 ОК 1-10 ЛР 1-11, КК1, КК2	МДК.01.05. Эксплуатация компьютерных сетей	196	60	166	60	-	24	-	6

	Производственная практика (по профилю специальности), часов	180	180				180	
	Всего	760	366	458	186	108	180	14

3.2. Тематический план и содержание профессионального модуля (ПМ)

ПМ. 01 Участие в планировании и организации работ по обеспечению защиты объекта

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся, курсовая работа	Объем, ак. ч / в том числе в форме практической подготовки, ак. ч
1	2	3
Раздел ПМ. 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		
МДК 01.01 Операционные системы		78/36
Раздел 1. Элементы теории операционных систем. Свойства операционных систем		34
Тема 1.1. Основы теории операционных систем	Содержание	2
	Тема 1.1.1 Определение операционной системы. Основные понятия. История развития операционных систем. Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.	2
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	Содержание	12
	В том числе практических занятий и лабораторных занятий	8
	Тема 1.2.1 Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС. Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.	2
	Тема 1.2.2 Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.	2
	Практическое занятие №1 (в форме практической подготовки) Тема 1.2.3 Виртуальные машины. Создание, модификация, работа.	2

	Практическое занятие №2 (в форме практической подготовки) Тема 1.2.4 Установка ОС.	2
	Практическое занятие №3 (в форме практической подготовки) Тема 1.2.5 Создание и изучение структуры разделов жесткого диска.	2
	Практическое занятие №4 (в форме практической подготовки) Тема 1.2.6 Операции с файлами.	2
Тема 1.3. Модульная структура операционных систем, пространство пользователя	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.3.1 Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.	2
	Практическое занятие №5 (в форме практической подготовки) Тема 1.3.2 Работа в консольном и графическом режимах	2
Тема 1.4. Управление памятью	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.4.1 Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти	2
	Практическое занятие №6 (в форме практической подготовки) Тема 1.4.2 Мониторинг за использованием памяти	2
Тема 1.5. Управление процессами, многопроцессорные системы	Содержание	6
	В том числе практических занятий и лабораторных занятий	4
	Тема 1.5.1 Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие. Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	2
	Практическое занятие №7 (в форме практической подготовки) Тема 1.5.2 Управление процессами	2

	Практическое занятие №8 (в форме практической подготовки) Тема 1.5.3 Наблюдение за использованием ресурсов системы	2
Тема 1.6. Виртуализация и облачные технологии	Содержание	6
	В том числе практических занятий и лабораторных занятий	4
	Тема 1.6.1 Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования. Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	2
	Практическое занятие №9 (в форме практической подготовки) Тема 1.6.2. Изучение примеров виртуальных машин (VBox)	2
	Практическое занятие №10 (в форме практической подготовки) Тема 1.6.3. Изучение примеров виртуальных машин (VMware)	2
		22
		22
Тема 2.1. Принципы построения защиты информации в операционных системах	Содержание	22
	В том числе практических занятий и лабораторных занятий	6
	Тема 2.1.1 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.	2
	Тема 2.1.2 Порядок обеспечения безопасности информации при эксплуатации операционных систем	2
	Тема 2.1.3 Типовые средства защиты информации в операционных системах	2
	Тема 2.1.4 Встроенный в Microsoft Windows межсетевой экран Брандмауэр Windows	2
	Тема 2.1.5 Сканер системы Windows Defender	2
Тема 2.1.6 Планирование систем и их приемка	2	

	Тема 2.1.7 Шифрование сменных носителей информации	2
	Тема 2.1.8 Использование правил политики безопасности «Deny write access to removable drives not protected BitLocker»	2
	Практическое занятие №11 (в форме практической подготовки) Тема 2.1.9 Управление учетными записями пользователей и доступом к ресурсам	2
	Практическое занятие №12 (в форме практической подготовки) Тема 2.1.10 Аудит событий системы	2
	Практическое занятие №13 (в форме практической подготовки) Тема 2.1.11 Изучение штатных средств защиты информации в операционных системах	2
Раздел 3. Особенности работы в современных операционных системах		22
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	Содержание	6
	В том числе практических занятий и лабораторных занятий	4
	Тема 3.1.1 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.	2
	Практическое занятие №14 (в форме практической подготовки) Тема 3.1.2 Создание дистрибутива Linux. Установка.	2
	Практическое занятие №15 (в форме практической подготовки) Тема 3.1.3 Работа в ОС Linux.	2
		10
Тема 3.2. Операционная система Windows	Содержание	10
	В том числе практических занятий и лабораторных занятий	2
	Тема 3.2.1 Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	2
	Тема 3.2.2 Виды политик управления доступом и информационными	2

	потоками применительно к операционным системам	
	Тема 3.2.3 Формы инструктажа пользователей по порядку работы в операционных системах	2
	Тема 3.2.4 Методы инструктажа пользователей по порядку работы в операционных системах	2
	Практическое занятие №16 (в форме практической подготовки) Тема 3.2.5 Установка и первичная настройка Windows.	2
Тема 3.3. Серверные операционные системы	Содержание	6
	В том числе практических занятий и лабораторных занятий	4
	Тема 3.3.1 Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	2
	Практическое занятие №17 (в форме практической подготовки) Тема 3.3.2 Работа с сетевой файловой системой.	2
	Практическое занятие №18 (в форме практической подготовки) Тема 3.3.3 Работа с серверной ОС, например, AltLinux.	2
	Промежуточная аттестация по МДК.01.01 в форме экзамена	
МДК 01.02 Базы данных		78/40
Раздел 1. Основы теории баз данных		6
Тема 1.1. Основные понятия теории баз данных. Модели данных	Содержание	1
	Тема 1.1.1 Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования. Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных. Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	1
Тема 1.2. Основы реляционной алгебры	Содержание	3

	В том числе практических занятий и лабораторных занятий	2
	Тема 1.2.1 Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	1
	Практическое занятие №1 (в форме практической подготовки)	2
	Тема 1.2.2 Операции над отношениями	1
Тема 1.3. Базовые понятия и классификация систем управления базами данных	Содержание	1
	Тема 1.3.1 Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору)	1
Тема 1.4. Целостность данных как ключевое понятие баз данных	Содержание	1
	Тема 1.4.1 Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	1
Раздел 2. Проектирование баз данных		12
Тема 2.1. Информационные модели реляционных баз данных	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.1.1 Типы информационных моделей. Логические модели данных. Физические модели данных.	2
	Практическое занятие №2 (в форме практической подготовки)	2
	Тема 2.1.2 Проектирование инфологической модели данных	2
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.2.1 Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам. Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.	2
	Практическое занятие №3 (в форме практической подготовки)	2
	Тема 2.2.2 Проектирование структуры базы данных	

Тема 2.3. Средства автоматизации проектирования	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.3.1 CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	2
	Практическое занятие №4 (в форме практической подготовки) Тема 2.3.2 Проектирование базы данных с использованием CASE-средств	2
Раздел 3. Организация баз данных		8
Тема 3.1. Создание базы данных. Манипулирование данными.	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 3.1.1 Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.	2
	Практическое занятие №5 (в форме практической подготовки) Тема 3.1.2 Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	2
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 3.2.1 Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	2
	Практическое занятие №6 (в форме практической подготовки) Тема 3.2.2 Создание взаимосвязей. Сортировка, поиск и фильтрация данных. Способы объединения таблиц	2
Раздел 4. Управление базой данных с помощью		10

SQL		
Тема 4.1. Структурированный язык запросов SQL.	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 4.1.1 Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	2
	Практическое занятие №7 (в форме практической подготовки)	
	Тема 4.1.2 Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL	2
Тема 4.2. Операторы и функции языка SQL	Содержание	6
	В том числе практических занятий и лабораторных занятий	4
	Тема 4.2.1 Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	2
	Практическое занятие №8 (в форме практической подготовки)	
	Тема 4.2.2 Создание и использование запросов. Группировка и агрегирование данных	2
	Практическое занятие №9 (в форме практической подготовки)	
	Тема 4.2.3 Коррелированные вложенные запросы. Создание в запросах вычисляемых полей. Использование условий	2
Раздел 5. Организация распределённых баз данных		20
Тема 5.1. Архитектуры распределённых баз данных	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 5.1.1 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, распределённые базы данных, параллельная обработка данных. Отличия и преимущества удалённых баз данных от локальных баз данных.	2

	Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.	
Тема 5.2. Серверная часть распределенной базы данных	Практическое занятие №10 (в форме практической подготовки) Тема 5.1.2 Управление доступом к объектам базы данных	2
	Содержание	12
	В том числе практических занятий и лабораторных занятий	2
	Тема 5.2.1 Планирование и развёртывание СУБД для работы с клиентскими приложениями	2
	Тема 5.2.3 Порядок настройки программного обеспечения систем управления базами данных и средств электронного документооборота	2
	Тема 5.2.4 Методы установки ПО рабочих станций и сервера	2
	Тема 5.2.5 Проверка работоспособности системы	2
	Тема 5.2.6 Восстановление работоспособности системы	2
	Практическое занятие №11 (в форме практической подготовки) Тема 5.2.7 Установка СУБД. Настройка компонентов СУБД.	2
	Содержание	4
Тема 5.3. Клиентская часть распределенной базы данных	В том числе практических занятий и лабораторных занятий	2
	Тема 5.3.1 Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация. Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа. Оптимизация производительности работы СУБД. Оптимизация работоспособности системы	2
	Практическое занятие №12 (в форме практической подготовки) Тема 5.3.2 Создание форм и отчетов. Создание меню. Генерация, запуск. Профилирование запросов клиентских приложений	2
Раздел 6. Администрирование и безопасность		22

Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	Содержание	8
	В том числе практических занятий и лабораторных занятий	6
	Тема 6.1.1 Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти. Настройка работоспособности системы управления базами данных.	2
	Практическое занятие №13 (в форме практической подготовки) Тема 6.1.2 Разработка хранимых процедур и триггеров	2
	Практическое занятие №14 (в форме практической подготовки) Тема 6.1.3 Выполнение настройки параметров работы программного обеспечения, включая системы управления базами данных	2
	Практическое занятие №15 (в форме практической подготовки) Тема 6.1.4 Выполнение настройки параметров работы программного обеспечения, средства электронного документооборота	2
		1
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	Содержание	
	Тема 6.2.1 Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	1
Тема 6.3. Механизмы защиты информации в системах управления базами данных		9
	Содержание	8
	В том числе практических занятий и лабораторных занятий Тема 6.3.1 Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и	1

	доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Средства защиты информации в базах данных	
	Практическое занятие №16 (в форме практической подготовки) Тема 6.3.2 Управление правами доступа к базам данных	2
	Практическое занятие №17 (в форме практической подготовки) Тема 6.3.3 Работа с программным обеспечением с соблюдением действующих требований по защите информации	2
	Практическое занятие №18 (в форме практической подготовки) Тема 6.3.4 Контроль процесса управления учетными записями пользователей СУБД	2
	Практическое занятие №19 (в форме практической подготовки) Тема 6.3.5 Контроль неизменности настроек средств защиты информации	2
Тема 6.4. Копирование и перенос данных. Восстановление данных	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 6.4.1 Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных	2
	Практическое занятие №20 (в форме практической подготовки) Тема 6.4.2 Аудит данных с помощью средств СУБД и триггеров. Резервное копирование и восстановление баз данных	2
Промежуточная аттестация по МДК.01.02 в форме экзамена		6
Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении		
МДК.01.03 Сети и системы передачи информации		42/20
Раздел 1. Теория телекоммуникационных сетей		14

Тема 1.1. Основные понятия и определения	Содержание	4
	Тема 1.1.1 Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	4
Тема 1.2. Принципы передачи информации в сетях и системах связи	Содержание	4
	Тема 1.2.1 Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	4
Тема 1.3. Типовые каналы передачи и их характеристики	Содержание	6
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.3.1 Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плездохронных систем передачи. Основные параметры и характеристики сигналов. Упрощенная схема организации канала ТЧ	4
	Практическое занятие №1 (в форме практической подготовки)	2
	Тема 1.3.2 Расчет пропускной способности канала связи	2
Раздел 2. Сети передачи данных		28
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	Содержание	20
	В том числе практических занятий и лабораторных занятий	16
	Тема 2.1.1 Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи.	2
	Протоколы и интерфейсы управления каналами и сетью передачи данных.	2
	Практическое занятие №2 (в форме практической подготовки)	2
	Тема 2.1.2 Конфигурирование сетевого интерфейса рабочей станции	2
	Практическое занятие №3 (в форме практической подготовки)	2
	Тема 2.1.3 Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP	2
Практическое занятие №4 (в форме практической подготовки)	2	
Тема 2.1.4 Коррекция проблем интерфейса маршрутизатора на физическом	2	

	и канальном уровне	
	Практическое занятие №5 (в форме практической подготовки) Тема 2.1.5 Диагностика и разрешение проблем сетевого уровня	2
	Практическое занятие №6 (в форме практической подготовки) Тема 2.1.6 Диагностика и разрешение проблем протоколов транспортного уровня	2
	Практическое занятие №7 (в форме практической подготовки) Тема 2.1.7 Диагностика и разрешение проблем протоколов прикладного уровня	2
	Практическое занятие №8 (в форме практической подготовки) Тема 2.1.8 Работа в компьютерных сетях с соблюдением действующих требований по защите информации. Конфигурация и контроль корректности настройки программно-аппаратных средств защиты информации в компьютерных сетях	2
	Практическое занятие №9 (в форме практической подготовки) Тема 2.1.9 Мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях. Обоснование выбора используемых программно-аппаратных средств защиты информации в компьютерных сетях	2
Тема 2.2. Беспроводные системы передачи данных	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.2.1 Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	2
	Практическое занятие №10 (в форме практической подготовки) Тема 2.2.2 Настройка Wi-Fi маршрутизатора	2
Тема 2.3. Сотовые и спутниковые системы	Содержание	2
	Тема 2.3.1 Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.	2

Промежуточная аттестация по МДК.01.03 в форме дифференцированного зачета		2
МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		94/30
Раздел 1. Разработка защищенных автоматизированных (информационных) систем		48
Тема 1.1. Основы информационных систем как объекта защиты.	Содержание	8
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.1.2 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.	4
	Тема 1.1.2 Основные особенности современных проектов АИС. Электронный документооборот.	2
	Практическое занятие №1 (в форме практической подготовки) Тема 1.1.3 Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	2
		10
Тема 1.2. Жизненный цикл автоматизированных систем	Содержание	4
	В том числе практических занятий и лабораторных занятий	4
	Тема 1.2.1 Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.	2

	Тема 1.2.2 Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.	2
	Тема 1.3.2 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.	2
	Практическое занятие №2 (в форме практической подготовки) Тема 1.3.3 Разработка технического задания на проектирование автоматизированной системы	2
	Практическое занятие №3 (в форме практической подготовки) Тема 1.3.4 Разработка технического задания на создание подсистем информационной безопасности автоматизированных систем	2
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	Содержание	10
	В том числе практических занятий и лабораторных занятий	6
	Тема 1.3.1 Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации	2
	Тема 1.3.2 Понятие уязвимости угрозы. Классификация уязвимостей.	2
	Практическое занятие №4 (в форме практической подготовки) Тема 1.3.3 Категорирование информационных ресурсов	2
	Практическое занятие №5 (в форме практической подготовки) Тема 1.3.4 Анализ угроз безопасности информации	2
	Практическое занятие №6 (в форме практической подготовки) Тема 1.3.5 Построение модели угроз	2
	Содержание	4
	Тема 1.4.1 Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	2
Тема 1.4. Основные меры защиты информации в автоматизированных системах		

	Тема 1.4.2 Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	2
		10
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	Содержание	
	Тема 1.5.1 Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа. Ограничение программной среды. Защита машинных носителей информации	2
	Тема 1.5.2 Регистрация событий безопасности. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	2
	Тема 1.5.3 Обнаружение (предотвращение) вторжений Контроль (анализ) защищенности информации Обеспечение целостности информационной системы и информации Обеспечение доступности информации	2
	Тема 1.5.4 Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	2
	Тема 1.5.5 Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных. Резервное копирование и восстановление данных.	2
Тема 1.6. Защита информации в распределенных автоматизированных системах	Содержание	
	Тема 1.6.1 Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	2

Тема 1.7. Особенности разработки информационных систем персональных данных	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.7.1 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
	Практическое занятие №7 (в форме практической подготовки) Тема 1.7.2 Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	2
Раздел 2.Эксплуатация защищенных автоматизированных систем.		46
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Содержание	6
	Тема 2.1.1 Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	2
	Тема 2.1.2 Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	2
	Тема 2.1.3 Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	2
Тема 2.2. Администрирование автоматизированных систем	Содержание	2
	Тема 2.2.1 Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	2
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном	Содержание	2
	Тема 2.3.1 Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем	2

исполнении	безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	
Тема 2.4. Защита от несанкционированного доступа к информации	Содержание	6
	Тема 2.4.1 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.	2
	Тема 2.4.2 Классификация автоматизированных систем. Требования по защите информации от НСД для АС	2
	Тема 2.4.3 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	2
Тема 2.5. СЗИ от НСД	Содержание	8
	В том числе практических занятий и лабораторных занятий	12
	Тема 2.5.1 Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.	2
	Тема 2.5.2 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.	2
	Тема 2.5.3 Обеспечение целостности информационной системы и информации	2
Тема 2.5.4 Централизованное управление системой защиты,	2	

	<p>Тема 2.6.2 Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении.</p> <p>Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам</p>	2
	<p>Практическое занятие №14 (в форме практической подготовки)</p> <p>Тема 2.6.3 Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем</p>	2
Тема 2.7. Документация на защищаемую автоматизированную систему	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.7.1 Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	2
	<p>Практическое занятие №15 (в форме практической подготовки)</p> <p>Тема 2.7.2 Оформление основных эксплуатационных документов на автоматизированную систему.</p>	2
Промежуточная аттестация по МДК.01.04 в форме экзамена		6
МДК.01.05. Эксплуатация компьютерных сетей		166/60
Раздел 1. Основы передачи данных в компьютерных сетях		40
Тема 1.1. Модели сетевого взаимодействия	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.1.1 Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI. Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	2
	<p>Практическое занятие №1 (в форме практической подготовки)</p> <p>Тема 1.1.2 Изучение элементов кабельной системы:</p>	2

	оперативный мониторинг и аудит безопасности	
	Практическое занятие №8 (в форме практической подготовки) Тема 2.5.5 Установка и настройка СЗИ от НСД	2
	Практическое занятие №9 (в форме практической подготовки) Тема 2.5.6 Защита входа в систему (идентификация и аутентификация пользователей). Разграничение доступа к устройствам. Управление доступом	2
	Практическое занятие №10 (в форме практической подготовки) Тема 2.5.7 Использование принтеров для печати конфиденциальных документов. Контроль печати	2
	Практическое занятие №11 (в форме практической подготовки) Тема 2.5.8 Настройка системы для задач аудита. Настройка контроля целостности и замкнутой программной среды. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	2
	Практическое занятие №12 (в форме практической подготовки) Тема 2.5.9 Исследование эффективности проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности	2
	Практическое занятие №13 (в форме практической подготовки) Тема 2.5.10 Работа с программным обеспечением с соблюдением действующих требований по защите информации	2
	Содержание	6
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	В том числе практических занятий и лабораторных занятий	2
	Тема 2.6.1 Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	2

	Элементы кабельной системы, защищенные от НСД	
Тема 1.2. Физический уровень модели OSI	Содержание	8
	В том числе практических занятий и лабораторных занятий	4
	Тема 1.2.1 Понятие линии и канала связи. Сигналы. Основные характеристики канала связи. Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.	2
	Тема 1.2.2 Оптоволоконные линии связи Стандарты кабелей. Электрическая проводка. Беспроводная среда передачи.	2
	Практическое занятие №2 (в форме практической подготовки) Тема 1.2.3 Создание сетевого кабеля на основе неэкранированной витой пары (UTP). Сварка оптического волокна: Оптимальность выбора аппаратных средств защиты информации	2
	Практическое занятие №3 (в форме практической подготовки) Тема 1.2.4 Оценка режимов выбора аппаратных средств защиты информации функционирования в компьютерных сетях	2
Тема 1.3. Топология компьютерных сетей	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.3.1 Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.	2
	Практическое занятие №4 (в форме практической подготовки) Тема 1.3.2 Разработка топологии сети небольшого предприятия. Построение одноранговой сети: Применение программно-аппаратных средств защиты информации в компьютерных сетях	2
Тема 1.4. Технологии Ethernet	Содержание	8
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.4.1 Обзор технологий построения локальных сетей.	2

	Тема 1.4.2 Технология Ethernet. Физический уровень.	2
	Тема 1.4.3 Технология Ethernet. Канальный уровень	2
	Практическое занятие №5 (в форме практической подготовки)	
	Тема 1.4.4 Изучение адресации канального уровня. MAC-адреса: Настройка правил фильтрации пакетов в компьютерных сетях	2
Тема 1.5. Технологии коммутации	Содержание	6
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.5.1 Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	2
	Тема 1.5.2 Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети. Технология PoweroverEthernet	2
	Практическое занятие №6 (в форме практической подготовки)	
	Тема 1.5.3 Создание коммутируемой сети: Правила фильтрации пакетов в компьютерных сетях	2
Тема 1.6. Сетевой протокол IPv4	Содержание	6
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.6.1 Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.	2
	Тема 1.6.2 Маршрутизация пакетов IPv4. Протоколы динамической маршрутизации	2
	Практическое занятие №7 (в форме практической подготовки)	
	Тема 1.6.3 Изучение IP-адресации: Настройка правил фильтрации пакетов в компьютерных сетях с применением IPv4	2
Тема 1.7. Скоростные и беспроводные сети	Содержание	4
	В том числе практических занятий и лабораторных занятий	2
	Тема 1.7.1 Сеть FDDI. Сеть 100VG-AnyLAN	2

	Сверхвысокоскоростные сети Беспроводные сети	
	Практическое занятие №8 (в форме практической подготовки) Тема 1.7.2 Настройка беспроводного сетевого оборудования: Оценка оптимальности выбора аппаратных средств защиты информации	2
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet		70
Тема 2.1. Основы коммутации	Содержание	8
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.1.1 Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах.	2
	Тема 2.1.2 Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов	2
	Тема 2.1.3 Состав типовых конфигураций коммутаторов для обеспечения безопасного функционирования	2
	Практическое занятие №9 (в форме практической подготовки) Тема 2.1.4 Работа с основными командами коммутатора: Настройка правил фильтрации пакетов и преобразование сетевых адресов	2
Тема 2.2. Начальная настройка коммутатора	Содержание	8
	В том числе практических занятий и лабораторных занятий	4
	Тема 2.2.1 Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.	2
	Тема 2.2.2 Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.	2
	Практическое занятие №10 (в форме практической подготовки) Тема 2.2.3 Команды обновления программного обеспечения коммутатора и	2

	сохранения/восстановления конфигурационных файлов: Настройка правил фильтрации пакетов с использованием NAT	
	Практическое занятие №11 (в форме практической подготовки) Тема 2.2.4 Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы: Настройка правил фильтрации пакетов с использованием скрытого NAT	2
Тема 2.3. Виртуальные локальные сети (VLAN)	Содержание	8
	В том числе практических занятий и лабораторных занятий	4
	Тема 2.3.1 Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.	2
	Тема 2.3.2 Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция Traffic Segmentation	2
	Практическое занятие №12 (в форме практической подготовки) Тема 2.3.3 Настройка VLAN на основе стандарта IEEE 802.1Q. Настройка протокола GVRP. Настройка сегментации трафика без использования VLAN: Предложения по применению программных средств защиты информации в компьютерных сетях	2
	Практическое занятие №13 (в форме практической подготовки) Тема 2.3.4 Настройка функции Q-in-Q (Double VLAN). Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.: Предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях	2
Тема 2.4. Функции повышения надежности и производительности	Содержание	8
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.4.1 Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.	2
	Тема 2.4.2 Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.	2

	<p>Тема 2.4.3 Дополнительные функции защиты от петель. Агрегирование каналов связи</p>	2
<p>Тема 2.5. Адресация сетевого уровня и маршрутизация</p>	<p>Практическое занятие №14 (в форме практической подготовки) Тема 2.4.4 Настройка протоколов связующего дерева STP, RSTP, MSTP. Настройка функции защиты от образования петель LoopBackDetection. Агрегирование каналов: Настройка правила SpanningTreeProtocol в компьютерных сетях</p>	2
	<p>Содержание</p>	10
	<p>В том числе практических занятий и лабораторных занятий</p>	4
	<p>Тема 2.5.1 Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса. Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.</p>	2
	<p>Тема 2.5.2 Планирование подсетей IPv6. Протокол NDP.</p>	2
	<p>Тема 2.5.3 Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.</p>	2
	<p>Практическое занятие №15 (в форме практической подготовки) Тема 2.5.4 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.: Правильность выбора аппаратно-программных средств защиты</p>	2
	<p>Практическое занятие №16 (в форме практической подготовки) Тема 2.5.5 Конфигурирование функции маршрутизатора NAT/PAT. Конфигурирование PPP и CHAP: Предложения по применению средств защиты информации в режиме функционирования</p>	2

Тема 2.6. Качество обслуживания (QoS)	Содержание	6
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.6.1 Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	2
	Тема 2.6.2 Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.	2
	Практическое занятие №17 (в форме практической подготовки) Тема 2.6.3 Настройка QoS. Приоритизация трафика. Управление полосой пропускания: Настройка правил фильтрации пакетов в модели QoS	2
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	Содержание	6
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.7.1 Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.	2
	Тема 2.7.2 Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.	2
	Практическое занятие №18 (в форме практической подготовки) Тема 2.7.3 Списки управления доступом (AccessControlList). Контроль над подключением узлов к портам коммутатора. Функция PortSecurity. Функция IP-MAC-Port Binding: Управление количеством подключаемых к портам коммутатора пользователей	2
Тема 2.8. Многоадресная рассылка	Содержание	2
	В том числе практических занятий и лабораторных занятий	2
	Тема 2.8.1 Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.	2
	Тема 2.8.2 Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping). Функция IGMP	2

	FastLeave.	
	Практическое занятие №19 (в форме практической подготовки) Тема 2.8.3 Отслеживание трафика многоадресной рассылки. Отслеживание трафика Multicast: IGMP snooping	2
Тема 2.9. Функции управления коммутаторами	Содержание	8
	В том числе практических занятий и лабораторных занятий	4
	Тема 2.9.1 Управление множеством коммутаторов. Протокол SNMP.	2
	Тема 2.9.2 RMON (Remote Monitoring). Функция Port Mirroring.	2
	Практическое занятие №20 (в форме практической подготовки) Тема 2.9.3 Функции анализа сетевого трафика: Работа со снифферами	2
	Практическое занятие №21 (в форме практической подготовки) Тема 2.9.4 Настройка протокола управления топологией сети LLDP: Стандарт IEEE 802.1AB-2009	2
Раздел 3. Межсетевые экраны		50
Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	Содержание	8
	Тема 3.1.1 Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.	2
	Тема 3.1.2 Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.	2
	Тема 3.1.3 Типовые конфигурации программно-аппаратных средств защиты информации	2
	Тема 3.1.4 Режимы функционирования программно-аппаратных средств защиты информации в компьютерных сетях	2
Тема 3.2. Межсетевые экраны	Содержание	26
	В том числе практических занятий и лабораторных занятий	10
	Тема 3.2.1 Технологии межсетевых экранов. Политика меж сетевого экрана. Межсетевые экраны с возможностями NAT.	4

	Тема 3.2.2 Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.	2
	Тема 3.2.3 Порядок реализации методов межсетевого экранирования	2
	Тема 3.2.4 Управляемые коммутаторы	2
	Тема 3.2.5 Порядок реализации программных средств межсетевого экранирования	2
	Тема 3.2.6 Порядок реализации программно-аппаратных средств межсетевого экранирования	2
	Тема 3.2.7 Организация эффективной работы средств межсетевого экранирования	2
	Практическое занятие №22 (в форме практической подготовки) Тема 3.2.8 Основы администрирования межсетевого экрана: Фильтрация трафика между сетями или узлами сети	2
	Практическое занятие №23 (в форме практической подготовки) Тема 3.2.9 Соединение двух локальных сетей межсетевыми экранами: Фильтрация трафика на основе MAC-адресов	2
	Практическое занятие №24 (в форме практической подготовки) Тема 3.2.10 Создание политики без проверки состояния: Персональные межсетевые экраны	2
	Практическое занятие №25 (в форме практической подготовки) Тема 3.2.11 Создание политик для традиционного (или исходящего) NAT: Правила фильтрования с использованием NAT	2
	Практическое занятие №26 (в форме практической подготовки) Тема 3.2.12 Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing: NAT in VoIP	2
	Содержание	16
Тема 3.3.		
Системы обнаружения и предотвращения проникновений	В том числе практических занятий и лабораторных занятий	6
	Тема 3.3.1 Основное назначение IDPS. Способы классификации IDPS.	2

	Выбор IDPS. Дополнительные инструментальные средства.	
	Тема 3.3.2 Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.	2
	Тема 3.3.3 Виды политик управления доступом в компьютерных сетях	2
	Тема 3.3.4 Виды политик управления информационными потоками в компьютерных сетях	2
	Тема 3.3.5 Пассивные и активные системы обнаружения вторжений	2
	Практическое занятие №27 (в форме практической подготовки) Тема 3.3.6 Обнаружение и предотвращение вторжений: Настройка Сетевой Системы обнаружения вторжений	2
	Практическое занятие №28 (в форме практической подготовки) Тема 3.3.7 Настройка Сетевой Системы обнаружения вторжений, основанной на прикладных протоколах APIDS	2
	Практическое занятие №29 (в форме практической подготовки) Тема 3.3.8 Блокирование атаки с помощью межсетевого экрана	2
Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	Содержание	8
	В том числе практических занятий и лабораторных занятий	2
	Тема 3.4.1 Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.	2
	Тема 3.4.2 Альтернативные таблицы маршрутизации. Правила выбора таблиц.	2
	Тема 3.4.3 Ограничение (шейпинг) трафика	2
	Практическое занятие №30 (в форме практической подготовки) Тема 3.4.5 Создание альтернативных маршрутов с использованием статической маршрутизации.	2
	Оценка оптимального выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях	
Промежуточная аттестация по МДК.01.05 в форме экзамена		6

Примерная тематика самостоятельной работы

1. Создание виртуальной машины. Установка операционной системы.
2. Подготовка рефератов по теме «Организация и использование механизмов защиты базы данных».
3. Настройка Wi-Fi маршрутизатора. Конфигурирование сетевого интерфейса
4. Разработка концепции защиты автоматизированной (информационной) системы.
5. Физическое кодирование с использованием манчестерского кода
6. Логическое кодирование с использованием скремблирования
7. Подключение клиента к беспроводной сети в инфраструктурном режиме.

Тематика домашних заданий

1. Изучение аналитических обзоров в области построения систем безопасности операционных систем
2. Выполнение индивидуального задания по теме «Проектирование инфологической модели базы данных».
3. Выполнение индивидуального задания по теме «Нормализация отношений».
4. Подготовка рефератов на тему «Развитие СУБД» (конкретной СУБД).
5. Выполнение индивидуального задания по теме «Создание базы данных. Создание таблиц. Организация межтабличных связей»
6. Выполнение индивидуального задания по теме «Организация запросов».
7. Выполнение индивидуального задания по теме «Создание пользовательского приложения средствами СУБД».
8. Разбор синтаксиса хранимых процедур и триггеров.
9. Изучение сетевых утилит
10. Конфигурирование сетевого интерфейса
11. Маршрутизация и управление потоками в сетях связи.
12. Анализ банка данных угроз безопасности информации
13. Анализ журнала аудита ОС на рабочем месте
14. Построение сводной матрицы угроз автоматизированной (информационной) системы
15. Анализ политик безопасности информационного объекта
16. Изучение аналитических обзоров в области построения систем безопасности
17. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации.
18. Физическое кодирование с использованием манчестерского кода
19. Логическое кодирование с использованием скремблирования
20. Подключение клиента к беспроводной сети в инфраструктурном режиме

<ul style="list-style-type: none"> 21. Оценка беспроводной линии связи 22. Проектирования беспроводной сети 23. Сбор информации о клиентских устройствах 24. Планирование производительности и зоны действия беспроводной сети 25. Предпроектное обследование места установки беспроводной сети 26. Обеспечение отказоустойчивости в беспроводных сетях 27. Режимы работы и организация питания точек доступа 28. Сегментация беспроводной сети 29. Настройка QoS 30. Постпроектное обследование и тестирование сети 31. Создание ACL-списка 32. Наблюдение за трафиком в сети VLAN 33. Определение уязвимых мест сети 34. Реализация функций обеспечения безопасности порта коммутатора 35. Исследование трафика 36. Создание структуры сети организации 37. Определение технических требований 38. Мониторинг производительности сети 39. Создание диаграммы логической сети 40. Подготовка к обследованию объекта 41. Обследование зоны беспроводной связи 42. Формулировка общих целей проекта 43. Разработка требований к сети 44. Анализ существующей сети 45. Определение характеристик сетевых приложений 	
<p>Учебная практика</p>	108
<ul style="list-style-type: none"> 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. 	

<ol style="list-style-type: none"> 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. 9. <i>Настройка программно-аппаратных средств защиты информации, в том числе антивирусной защиты в операционных системах по заданным шаблонам;</i> 10. <i>Инструктаж пользователей по порядку работы в операционных системах;</i> 11. <i>Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах;</i> 12. <i>Ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях;</i> 13. <i>Установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации</i> 	
<p>Производственная практика:</p>	<p>180</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 	

- | | |
|---|--|
| <ul style="list-style-type: none"> 16. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем 17. Настройка программно-аппаратных средств защиты информации, в том числе антивирусной защиты в операционных системах по заданным шаблонам; 18. Инструктаж пользователей по порядку работы в операционных системах; 19. Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах; 20. Ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях; 21. Установка средств межсетевое экранирования в соответствии с действующими требованиями по защите информации; 22. Инструктаж пользователей по порядку безопасной работы в компьютерных сетях; 23. Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях; 24. Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях. | |
|---|--|

Для характеристики уровня освоения учебного материала используются следующие обозначения:

- 1 - ознакомительный (узнавание ранее изученных объектов, свойств);
- 2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
- 3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к материально-техническому обеспечению

Реализация программы предполагает наличие учебного кабинета

Кабинет № 27 Лаборатория информационных технологий, программирования и баз данных

Оборудование:

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

4.2. Информационное обеспечение обучения

4.2.1. Основные источники

1. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью». Выпуск 2 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 130 с. — ISBN 978-5-9912-0272-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5179> (дата обращения: 11.07.2023). — Режим доступа: для авториз. пользователей.
2. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии:/С.А. Жданов Н.Ю. Иванова, В.Г Маняхина – М.: Издательский центр «Академия», 2014.-258 с. - ISBN 658-9-2568-3258-8 – Текст : непосредственный.
3. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации:/Б. В. Костров, В. Н Ручкин– М.: Издательский центр «Академия», 2016.-175 с. – ISBN 654-8-4468-7764-5— Текст : непосредственный.
4. Мельников Д. Информационная безопасность открытых систем.:/Д. Мельников. - М.: Форум, 2013.- 248 с. – ISBN 852-4-5691-7764-5- Текст : непосредственный.
5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание:/ В.Олифер, Н. Олифер– Питер, 2015.– ISBN 654-8-4468-7764-5 – Текст : непосредственный.
6. Сеницын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы:/ С.В. Сеницын, А.В. Батаев, Н.Ю. Налютин– М.: Издательский центр «Академия», 2013.- ISBN 128-8-4468-3258-9 – Текст : непосредственный.
7. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие:/ Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.– 416 с. – ISBN 567-8-4558-3258-2 - Текст : непосредственный.
8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд./ Э. Таненбаум, Д. Уэзеролл– Питер, 2013.– ISBN 978-5-4468-7764-5 – Текст : непосредственный.

4.2.2. Дополнительные источники:

9. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем.:/ А.А. Безбогов., А.В. ЯковлевМ. Гелиос АРВ, 2008.. – ISBN 456-5-4468-2878-5– Текст : непосредственный.
10. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. / М.А. БорисовМ.: Либроком, 2012. – 224 с. — ISBN 652-8-4468-3698-8 - Текст : непосредственный.
11. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. / В.Л. Бойдо2-е изд. - СПб: Питер, 2006 - 703 с.– ISBN 987-5-3355-7788-5 – Текст : непосредственный.
12. ГубенковА.А.Информационная безопасность вычислительных сетей: учеб.пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.- ISBN 852-8-4468-3258-5 – Текст : непосредственный.
13. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы./ Х. М.Дейтел, П. Дж.Дейтел, Д. Р.Чофнес– М.: Бином, 2011. – 1024 с.– ISBN 852-8-4468-3258-5– Текст : непосредственный.
14. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность:/ Х. М.Дейтел, П. Дж.Дейтел, Д. Р.Чофнес– М.: Бином, 2011. – 704 с.– ISBN 282-8-5856-6548-5 – Текст : непосредственный.
15. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.:/ В.И. Иванов, В.Н. Гордиенко, Г.Н. Попов М.: Горячая линия-Телеком., 2008– ISBN 2658-5-4468-454-5– Текст : непосредственный.
16. Кофлер М., Linux. Полное руководство – Питер, 2011. – 800 с.– ISBN 357-8-4468-3258-5– Текст : непосредственный.
17. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие:/ В.Г.Кулаков, М.В. ГагаринМ.: Радио и связь, 2008– ISBN 654-8-5679-3258-5– Текст : непосредственный.
18. Лапони́на О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. / О.Р. Лапони́наЛаборатория знаний, 2007.- 531 с.- ISBN 852-4-5691-7764-5 – Текст : непосредственный.
19. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд.:/ С. Мак-Клар, Дж.Скембрей, Д.Куртц – М.: Вильямс, 2004. – 656 с.– ISBN 5689-4468-7764-5 – Текст : непосредственный.
20. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов./ А.А.Малюк, С.В. Пазизин, Н.С. Погожин3-е изд., стер. М.: Горячая линия, 2005.- 147 с.– ISBN 8978-8899-7764-5– Текст : непосредственный.

21. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб.пос. для студентов СПО/ Т. Л.Партык, И. И. Попов. – М.: Форум, 2013. – 544 с.– ISBN 6657-4468-2365-5 – Текст : непосредственный.
22. 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.– ISBN 658-8-4558-3258-3– Текст : непосредственный.
23. Руссинович М., Соломон Д., Внутреннее устройство MicrosoftWindows. Основные подсистемы операционной системы:/ М.Руссинович,Д. Соломон– Питер, 2014. – 672 с.– ISBN 987-5-3355-7788-5 – Текст : непосредственный.
24. Северин В. Комплексная защита информации на предприятии. :/ В Северин. М.: Городец, 2008. – 368 с.– ISBN 652-8-4468-3698-8 – Текст : непосредственный.

4.2.3. Периодические издания:

25. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
26. Журналы Защита информации. Инсайд: Информационно-методический журнал
27. Информационная безопасность регионов: Научно-практический журнал
28. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности:URL: <http://cyberrus.com/>
29. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ.:URL: <http://bit.mephi.ru/>

4.2.4. Электронные источники:

30. Информационно-справочная система по документам в области технической защиты информации:URL: www.fstec.ru – Текст : электронный.
31. Информационный портал по безопасности:URL: www.SecurityLab.ru. – Текст : электронный.
32. Образовательные порталы по различным направлениям образования и тематике:URL: <http://derobr.gov35.ru/> – Текст : электронный.
33. Российский биометрический портал:URL: www.biometrics.ru – Текст : электронный.
34. Сайт журнала Информационна – Текст : электронный.я безопасность:URL: <http://www.itsec.ru> – – Текст : электронный.
35. Сайт Научной электронной библиотеки :URL: www.elibrary.ru – Текст : электронный.
36. Справочно-правовая система «Гарант» » :URL: www.garant.ru – Текст : электронный.
37. Справочно-правовая система «Консультант Плюс»:URL: www.consultant.ru – Текст : электронный.

38. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): URL: www.fstec.ru – Текст : электронный.
39. Федеральный портал «Информационно-коммуникационные технологии в образовании»: URL: <http://www.ict.edu.ru> – Текст : электронный.
40. Федеральный портал «Российское образование»: URL: www.edu.ru – Текст : электронный.

4.3. Общие требования к организации образовательного процесса.

Обязательным условием успешного освоения профессионального модуля «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» является обязательное прохождение производственной практики.

Производственная практика проводится концентрированно в организациях, направление деятельности которых соответствует профилю подготовки обучающихся. Предусматривается сдача дифференцированного зачета по производственной практике (по профилю специальности). Освоение каждого междисциплинарного курса завершается экзаменами и дифференцированным зачетом, а освоение программы профессионального модуля – проведением квалификационного экзамена.

4.4. Кадровое обеспечение образовательного процесса.

Требования к квалификации педагогических кадров, обеспечивающих обучение по профессиональному модулю Эксплуатация автоматизированных (информационных) систем в защищенном исполнении: наличие высшего профессионального образования, соответствующего профилю преподаваемого МДК. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального учебного цикла.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Образовательное учреждение, реализующее подготовку по программе профессионального модуля, обеспечивает организацию и проведение текущего и итогового контроля индивидуальных образовательных достижений – демонстрируемых обучающимися знаний, умений и навыков.

Текущий контроль проводится преподавателем в процессе обучения. Итоговый контроль проводится экзаменационной комиссией после обучения по междисциплинарному курсу.

Обучение по профессиональному модулю завершается промежуточной аттестацией, которую проводит экзаменационная комиссия. В состав экзаменационной комиссии могут входить представители общественных организаций обучающихся.

Формы и методы текущего и итогового контроля по профессиональному модулю самостоятельно разрабатываются образовательным учреждением и доводятся до сведения обучающихся не позднее начала двух месяцев от начала обучения.

Для текущего и итогового контроля образовательными учреждениями создаются фонды оценочных средств (ФОС).

ФОС включают в себя педагогические контрольно-измерительные материалы, предназначенные для определения соответствия (или несоответствия) индивидуальных образовательных достижений основным показателям результатов подготовки (таблицы).

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

<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>
<p>ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.</p>	<p>- участие в профориентационной работе; - участие в профессиональных конкурсах; - участие в научно-исследовательской работе.</p>	<p>- отчеты по итогам производственной (по профилю специальности) практики. - создание портфолио обучающихся. - отзывы научных руководителей.</p>

<p>ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.</p>	<ul style="list-style-type: none"> - планирование информационного поиска из широкого набора источников, необходимого для выполнения профессиональных задач; - проведение анализа полученной информации, выделяет в ней главные аспекты; структурировать отобранную информацию в соответствии с параметрами поиска; - интерпретация полученной информации в контексте профессиональной деятельности 	<p>Наблюдение и экспертная оценка на практических занятиях и при выполнении работ на учебной практике</p>
<p>ОК 3. Планировать и реализовывать собственное и личностное развитие.</p>	<ul style="list-style-type: none"> - использование актуальной нормативно-правовой документацию по специальности; - применение современной научной профессиональной терминологии; - определение траектории профессионального развития и самообразования 	<p>Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках</p>
<p>ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.</p>	<ul style="list-style-type: none"> - участие в деловом общении для эффективного решения деловых задач; - планирование профессиональной деятельности; - организация работы коллектива и команды; - взаимодействие с коллегами, руководством, клиентами в ходе профессиональной деятельности. 	<p>Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках</p>

<p>ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.</p>	<ul style="list-style-type: none"> - использование вербальных и невербальных способов коммуникации на государственном языке с учетом особенностей и различий социального и культурного контекста; - соблюдение норм публичной речи и регламента; - самостоятельный выбор стиля монологического высказывания (служебный доклад, выступление на совещании, презентация проекта и т.п.) в зависимости от его цели и целевой аудитории и с учетом особенностей и различий социального и культурного контекста; - создание продукта письменной коммуникации определенной структуры на государственном языке; - самостоятельный выбор стиля (жанра) письменной коммуникации на государственном языке в зависимости от цели, содержания и адресата. 	<p>Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках</p>
<p>ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.</p>	<ul style="list-style-type: none"> - осознание конституционных прав и обязанностей; - соблюдение закона и правопорядка. - участие в мероприятиях гражданского-патриотического характера, волонтерском движении. - аргументированное представление и отстаивание свое мнение с соблюдением этических норм и общечеловеческих ценностей. - осуществление своей деятельности на основе соблюдения этических норм и общечеловеческих ценностей; - демонстрацию 	<p>Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках</p>

	сформированности российской гражданской идентичности, патриотизма, уважения к своему народу, уважения к государственным символам (гербу, флагу, гимну).	
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	<ul style="list-style-type: none"> - обладание нормами экологической чистоты и безопасности. - осуществление деятельности по сбережению ресурсов и сохранению окружающей среды. - прогнозирование техногенные последствия для окружающей среды, бытовой и производственной деятельности человека; - прогнозирование возникновений опасных ситуаций по характерным признакам их появления, а также на основе анализа специальной информации, получаемой из различных источников; - владение приемами эффективных действий в опасных и чрезвычайных ситуациях природного, техногенного и социального характера. 	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	<ul style="list-style-type: none"> - классифицирование оздоровительных систем физического воспитания, направленных на укрепление здоровья, профилактику профессиональных заболеваний, вредных привычек и увеличения продолжительности жизни; - соблюдение норм здорового образа жизни, осознанное выполнение правил безопасности 	Наблюдение и экспертная оценка на практических занятиях и при выполнении работ на учебной практике

	<p>жизнедеятельности;</p> <ul style="list-style-type: none"> - составление своего индивидуального комплекса физических упражнений для поддержания необходимого уровня физической подготовленности; - организация собственной деятельности по укреплению здоровья и физической выносливости 	
<p>ОК 9. Использовать информационные технологии профессиональной деятельности.</p> <p>в</p>	<ul style="list-style-type: none"> - планирование информационного поиска; - принятие решения о завершении (продолжении) информационного поиска на основе оценки достоверности (противоречивости) полученной информации для решения профессиональных задач; - осуществление обмена информацией с использованием современного оборудования и программного обеспечения, в том числе на основе сетевого взаимодействия; - анализ информации, выделение в ней главных аспектов, структурирование, презентация. 	<p>Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках</p>
<p>ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.</p> <p>на и</p>	<ul style="list-style-type: none"> - изучение нормативно-правовой документации, технической профессиональной документации на государственном и иностранном языке, литературы и современных научных разработок в области будущей профессиональной деятельности на государственном языке; - применение необходимого лексического и грамматического минимума для чтения и перевода иностранных текстов профессиональной направленности; - владение современной научной и профессиональной 	<p>Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках</p>

	<p>терминологией;</p> <ul style="list-style-type: none">- самостоятельное совершенствование устной и письменной речи и пополнение словарного запаса;- владение навыками технического перевода текста, понимание содержания инструкций и графической документации на иностранном языке в области профессиональной деятельности.	
--	---	--