Минобрнауки России

ФГБОУ ВО «Тульский государственный университет»

Технический колледж имени С.И.Мосина

УТВЕРЖДАЮ
Заместитель директора колледжа
по учебной работе

_____ Д.А.Матвеева
«21» 01 2021 г.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.7 Технические средства информатизации

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

(базовая подготовка)

Тула 2021

РАССМОТРЕНА

Цикловой комиссией информационных технологий

Протокол от «14» мая 2021 г. № 6

Председатель цикловой комиссии _____ И.В.Миляева

Авторы: Романова Л.В., преподаватель Технического колледжа им.С.И.Мосина ТулГу

СОДЕРЖАНИЕ

1 Общая характеристика рабочей программы учебной дисциплины

1.1 Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к обязательной части профессионального цикла программы подготовки специалистов среднего звена и является общепрофессиональной.

Дисциплина базируется на знаниях, умениях и навыках, сформированных в ходе изучения предшествующих дисциплин: *ЕН.02 Информатика*.

1.2 Цель и планируемые результаты освоения дисциплины

Код ПК, ОК	Практический опыт	Умения	Знания
ОК1,ОК9 *ПК 1.4* *ПК 2.1* *ПК 2.5*	– компоновка и конфигурирование персонального компьютера; – инсталляция и настройка периферийного оборудования и программного обеспечения; – определение простейших неисправностей в работе компьютерной системы и их устранение	– пользоваться основными видами современной вычислительной техники, периферийных и мобильных устройств, и других технических средств информатизации; – правильно эксплуатировать и устранять типичные выявленные дефекты технических средств информатизации	– назначение и принципы работы основных узлов современных технических средств информатизации; – структурные схемы и порядок взаимодействия компонентов современных технических средств информатизации; – особенности организации ремонта и обслуживания компонентов технических средств информатизации; – функциональные и архитектурные особенности мобильных технических средств информатизации

Результат освоения рабочей программы учебной дисциплины *Архитектура компьютерных систем* влияет на формирование у обучающихся общих (ОК) и профессиональных (ПК) компетенций.

Код	Наименование результат обучения
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности
ПК 1.4	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК 2.5	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств

2 Структура и содержание учебной дисциплины

2.1 Объём учебной дисциплины и виды учебной работы

Вид учебной работы	*Объём часов*
Обязательная аудиторная учебная нагрузка в том числе: практические занятия уроки проверки знаний, умений	80 40 –
Самостоятельная работа	8
Промежуточная аттестация 1 семестр – экзамен	

2.2 Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объём часов	Осваиваемые элементы компетенций
1	2	3	4
Введение	*Содержание учебного материала*	*2*	*ОК 1, ОК9* *ПК 1.4* *ПК 2.1* *ПК 2.5*
	Роль и место дисциплины в профессиональной деятельности. Перечень разделов и тем. Рекомендации в изучении дисциплины. Требования, предъявляемые к обучающимся при изучении дисциплины. Рекомендуемые источники информации Назначение и основные этапы развития технических средств информатизации	2	
Раздел 1. Общая характеристика и классификация технических средств информатизации		**2**	
Тема 1.1 Классификация технических средств информатизации	*Содержание учебного материала*	*2*	*ОК 1,ОК9* *ПК 1.4* *ПК 2.1* *ПК 2.5*
	Области применения и важность использования технических средств информатизации. Способы классификации технических средств информатизации	2	
Раздел 2. Архитектура компьютерных систем		**20**	
Тема 2.1 Представление информации в вычислительных системах	*Содержание учебного материала*	*2*	*ОК 1,ОК9* *ПК 1.4* *ПК 2.1* *ПК 2.5*
	Системы счисления, используемые в вычислительной технике. Перевод чисел из одной системы счисления в другую Машинные коды Арифметические операции над двоичными числами с фиксированной и плавающей запятой	2	
	Практическая работа	*4*	
	Перевод чисел из одной системы счисления в другую		
	Арифметические операции над двоичными числами		

1	2	3	4
Тема 2.2 Архитектура и принципы работы основных логических блоков вычислительных систем	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Основные и универсальные логические операции. Законы алгебры логики. Техническая реализация логических функций. Типовые комбинационные и последовательностные логические устройства	2	
	Практическая работа	*4*	
	Логические выражения		
	Логические элементы		
	Самостоятельная работа по выполнению домашнего задания	*2*	
Тема 2.3 Основные подсистемы вычислительных систем	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Процессор Подсистема памяти Подсистема ввода-вывода Подсистема прерываний	2	
	Практическая работа	*2*	
	Основные подсистемы вычислительной техники		
	Самостоятельная работа по выполнению домашнего задания	*2*	
Раздел 3. Основные конструктивные элементы средств вычислительной техники		**40**	
Тема 3.1 Структура и стандарты шин	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Особенности организации взаимосвязи компонентов: сигналы и среда передачи; достоверность, надёжность передачи и управление потоком; способы передачи данных. Иерархия и организация подключений Печатные платы. Кабели и разъёмы. Свойства интерфейса. Методы повышения эффективности интерфейсов Виды интерфейсов: системные, периферийные, беспроводные, специализированные и вспомогательные	2	
	Практическая работа	*2*	
	Интерфейсы вычислительной техники		
Тема 3.2 Блоки питания системного блока персонального компьютера	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Корпуса компьютеров Блок питания: конструкция и принцип работы, параметры и спецификации, разъёмы. Критерии выбора	2	
Тема 3.3 Системные платы	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Форма-фактор. Архитектура и спецификации. Синхронизация и потоки данных. Критерии выбора	2	
	Практическая работа	*2*	
	Системная плата		
Тема 3.4 Центральный процессор	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Устройство. Основные технические характеристики. Идентификация и совместимость	2	
	Практическая работа	*2*	
	Процессор		
	Самостоятельная работа по выполнению домашнего задания	*2*	

1	2	3	4
Тема 3.5 Память компьютера	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Признаки классификации. Режимы работы и организация обращений. Типы и характеристики оперативной памяти	2	
	Практическая работа	*2*	
	Оперативная память		
Тема 3.6 Платы расширения	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Видеокарта Звуковая карта Сетевая карта	2	
	Практическая работа	*2*	
	Платы расширения		
Тема 3.7 Компоновка, модернизация и техническое обслуживание компьютерной системы	*Содержание учебного материала*	*4*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Конфигурация компьютерной системы Системные ресурсы	2	
	Принципы профилактического обслуживания Мониторинг и диагностика компьютерной системы Неисправности компьютерной системы	2	
	Практическая работа	*10*	
	Компоновка системного блока		
	Утилита CMOS Setup		
	Профилактическое обслуживание компьютерной системы		
	Диагностические программы		
	Аппаратные неисправности компьютерной системы		
	Самостоятельная работа по выполнению домашнего задания	*2*	
Раздел 4. Периферийные устройства вычислительной техники		**22**	
Тема 4.1 Дисковая подсистема	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Магнитная технология записи-чтения Оптическая технология записи-чтения Электрическая технология записи-чтения	2	
	Практическая работа	*2*	
	Конструкция и принцип работы устройств хранения данных		
Тема 4.2 Видеоподсистема	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Монитор с электронно-лучевой трубкой Монитор с жидкокристаллической матрицей Проекционный аппарат	2	
	Практическая работа	*2*	
	Конструкция и принцип работы устройств отображения данных		
Тема 4.3 Устройства подготовки и ввода информации	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Клавиатура Манипуляторные устройства Сенсорная панель Сканер	2	
	Практическая работа	*2*	
	Конструкция и принцип работы устройств интерактивного взаимодействия		

1	2	3	4
Тема 4.4 Печатающие устройства	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Фотоэлектронные принтеры Струйные принтеры Плоттеры	2	
	Практическая работа	*2*	
	Конструкция и принцип работы устройств вывода на печать		
Тема 4.5 Система обработки и воспроизведения аудиоинформации	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Устройства ввода звуковой информации Устройства вывода звуковой информации	2	
	Практическая работа	*2*	
	Конструкция и принцип работы устройств ввода-вывода звуковой информации		
Тема 4.6 Нестандартные устройства	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Цифровые камеры Измерительные приборы Бытовые приборы	2	
Раздел 5. Технические средства систем дистанционной передачи информации		**2**	
Тема 5.1 Структура и основные характеристики	*Содержание учебного материала*	*2*	*ОК 1,ОК9 ПК 1.4 ПК 2.1 ПК 2.5*
	Аппаратные средства компьютерных сетей	2	
	Всего:	**88**	

Самостоятельная работа обучающихся:

- систематическая проработка конспектов занятий и учебной литературы;
- подготовка к практическим занятиям и оформление отчёта по выполнению заданий;
- подготовка рефератов, докладов, презентаций.

3 Условия реализации программы учебной дисциплины

3.1 Требования к минимальному материально техническому обеспечению

Реализация программы дисциплины требует наличия кабинетов информатики, информационной безопасности, лаборатория программных и программно-аппаратных средств защиты информации

Оборудование кабинетов:
посадочные места по количеству обучающихся,
рабочие места с персональными компьютерами и сетевым оборудованием
рабочее место преподавателя,
мультимедиапроектор, экран, интерактивная доска,
программное обеспечение,
оргсредства, комплект демонстрационных стендов
наглядные стенды, схемы, плакаты, слайды

Оборудование лаборатории:

- рабочие места с персональными компьютерами и сетевым оборудованием, подключенными к локальной вычислительной сети и информационно-телекоммуникационной сети «Интернет»
- рабочее место преподавателя
- средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок (индикатор поля – частотомер, скоростной поисковый приемник, устройства защиты телефонных переговоров и слаботочных линий, устройства защиты сотовой связи, генератор акустического шума);
- средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.) (средства обнаружения каналов утечки информации, шумомер); стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов (стенд с системой контроля доступа, охранная и пожарная сигнализация);
- информационная доска для маркера;
- комплект демонстрационных стендов;
- программное обеспечение.

3.2 Информационное обеспечение обучения

Основные источники

1 Емельянов, В.А. ИТ-инфраструктура организации : учебное пособие / Емельянов В.А. — Москва : КноРус, 2019. — 144 с. — ISBN 978-5-406-05063-7. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/936958

2 Лошаков, С. Периферийные устройства вычислительной техники : учебное пособие / С. Лошаков. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 419 с. — ISBN 978-5-4497-0555-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/94858.html

Дополнительные источники

1 Горюшкин, А.А. Офисное программное обеспечение : практикум / Горюшкин А.А. — Москва : Русайнс, 2019. — 118 с. — ISBN 978-5-4365-3405-3. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/932149

2 Синаторов, С.В. Пакеты прикладных программ : учебное пособие / Синаторов С.В. — Москва : КноРус, 2020. — 195 с. — ISBN 978-5-406-08111-2. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/939069

3 Синаторов, С.В. Пакеты прикладных программ : учебное пособие / Синаторов С.В. — Москва : КноРус, 2020. — 195 с. — ISBN 978-5-406-08111-2. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/939069

4 Акимова, Е. В. Вычислительная техника : учебное пособие / Е. В. Акимова. — Санкт-Петербург : Лань, 2020. — 68 с. — ISBN 978-5-8114-4925-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/142354

Периодические издания

1 Системный администратор : [журнал]. - Москва, 2020.

2 Программирование : научный журнал / учредители : ФГБОУ ВО МГУ им. М.В.Ломоносова, РАН, Отделение информатики, вычислительной техники и автоматизации РАН. - Москва : Наука, 2020 - . - ISSN 0132-3474. - Текст : электронный // НЭБ eLibrary [сайт]. — URL: https://www.elibrary.ru/title_about_new.asp?id=7966

3 Информационно-управляющие системы : научный журнал / учредитель : ООО «Информационно[управляющие системы». - Санкт-Петербург : Изд-во Санкт-Петербургского государственного университета аэрокосмического приборостроения, 2020 - . - ISSN 1684-8853. - Текст : электронный // НЭБ eLibrary [сайт]. — URL: https://www.elibrary.ru/title_about.asp?id=25785

Интернет-ресурсы

ЭБС Юрайт. - Интернет- ссылка https://urait.ru/

ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/

ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/

ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/

НЭБ eLibrary. - Интернет-ссылка https://www.elibrary.ru/

4 Контроль и оценка результатов освоения учебной дисциплины

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

Результаты обучения		Критерии оценки	Формы и методы оценки
1		2	3
ОК 1,ОК9 *ПК 1.4* *ПК 2.1* *ПК 2.5*	*Знания:* – назначение и принципы работы основных узлов современных технических средств информатизации; – структурные схемы и порядок взаимодействия компонентов современных технических средств информатизации; – особенности организации ремонта и обслуживания компонентов технических средств информатизации; – функциональные и архитектурные особенности мобильных технических средств информатизации	Демонстрация знаний об информационно-логических основах вычислительной техники. Демонстрация знаний о принципах работы основных подсистем вычислительной техники. Демонстрация знаний о назначении, технических характеристиках, реализации разъёма, особенностях подключения Демонстрация знаний об особенностях организации ремонтно-профилактических работ технических средств информатизации	Контроль знаний выполняется по результатам проведения различных форм опроса, тестирования, выполнения практических заданий, выполнения контрольных работ, выполнение заданий для самостоятельной работы, промежуточной аттестации
	Умения: – пользоваться основными видами современной вычислительной техники, периферийных и мобильных устройств, и других технических средств информатизации; – правильно эксплуатировать и устранять типичные выявленные дефекты технических средств информатизации	Умение переводить число в различные системы счисления и машинные коды. Умение выполнять арифметические действия над двоичными числами. Умение определять параметры, используемые при организации взаимосвязи компонентов компьютерной системы. Умение определять тип интерфейса и его основные свойства. Умение определять неисправности в работоспособности компьютерной системы и устранять их	Контроль умений осуществляется в ходе выполнения практических заданий, выполнение заданий для самостоятельной работы, промежуточной аттестации

1		2	3
	Практический опыт: – компоновка и конфигурирование персонального компьютера; – инсталляция и настройка периферийного оборудования и программного обеспечения; – определение простейших неисправностей в работе компьютерной системы и их устранение	Правильность подключения и конфигурирования компонентов компьютерной системы Соблюдение этапов установки и обновления программного обеспечения Системный подход к поиску неполадок в работе компьютерной системы Демонстрация мер, необходимых для восстановления работоспособности компьютерной системы Соблюдение требований техники безопасности при работе с ВТ	Контроль практического опыта осуществляется в ходе выполнения практических заданий, выполнения контрольных работ, выполнение заданий для самостоятельной работы, промежуточной аттестации

Минобрнауки России
ФГБОУ ВО «Тульский государственный университет»
Технический колледж им. С.И. Мосина

УТВЕРЖДАЮ
Заместитель директора колледжа
по учебной работе

_____ **Д.А.Матвеева**
«21» января 2021 г.

РАБОЧАЯ ПРОГРАММА

профессионального модуля

ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

для специальности

10.02.05 Обеспечение информационной безопасности

автоматизированных систем

2021

РАССМОТРЕНА

цикловой комиссией информационных технологий

Протокол от «14» января 2021 № 6

Председатель цикловой комиссии _____ И.В. Миляева

СОДЕРЖАНИЕ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

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

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

1.1.2. Общие компетенции:

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

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

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; – администрирования автоматизированных систем в защищенном исполнении; – эксплуатации компонентов систем защиты информации автоматизированных систем; – диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении
уметь	– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности
знать	– состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; – принципы построения, физические основы работы периферийных устройств; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; – принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 792 часов, из них

на освоение МДК – 474 часа,

на самостоятельную работу 102 часа,

на промежуточную аттестацию 54 часа,

на практики – 162 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 1.1. ОК 1– ОК 10	**Раздел 1 модуля.** Установка и настройка автоматизированных (информационных) систем в защищенном исполнении	**208**	**172**	76	–		–	**36**
ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 10	**Раздел 2 модуля.** Администрирование автоматизированных (информационных) систем в защищенном исполнении	**368**	**302**	142	–		–	**66**
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	**162**					**162**	–
	Промежуточная аттестация							
	По МДК 01.01. экзамен в 2 семестре	**18**						
	По МДК 01.02. дифференцированный зачет во 2 семестре							
	По МДК 01.03. дифференцированный зачет во2 семестре, экзамен в 3 семестре	**18**						
	По МДК 01.04. дифференцированный зачет в 3 4 семестрах							
	По МДК 01.05. дифференцированный зачет в 3 4 семестрах							
	Экзамен по профессиональному модулю (экзамен квалификационный) в 4 семестре	**18**						
	Всего:	**792**	**474**	218	–	-	**162**	**102**

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов
1	2	3
Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении		**208**
МДК.01.01 Операционные системы		**76**
Раздел 1. Элементы теории операционных систем. Свойства операционных систем		**44**
Тема 1.1. Основы теории операционных систем	**Содержание**	**6**
	Определение операционной системы. Основные понятия. История развития операционных систем. Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.	
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	**Содержание**	**8**
	Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС.	
	Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.	
	Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.	
	Тематика практических занятий и лабораторных работ	**8**
	Виртуальные машины. Создание, модификация, работа	
	Установка ОС	
	Операции с каталогами и файлами	
Тема 1.3. Модульная структура	**Содержание**	**2**
	Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме.	

операционных систем, пространство пользователя	Оболочки операционных систем.	
	Тематика практических занятий и лабораторных работ	**2**
	Основные приемы работы в командной оболочке	
Тема 1.4. Управление памятью	**Содержание**	**2**
	Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти	
	Тематика практических занятий и лабораторных работ	**2**
	Мониторинг за использованием памяти	
Тема 1.5. Управление процессами, многопроцессорные системы	**Содержание**	**4**
	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие	
	Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	
	Тематика практических занятий и лабораторных работ	**4**
	Сбор сведений о системе. Управление процессами	
Тема 1.6. Виртуализация и облачные технологии	**Содержание**	**4**
	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования	
	Облачные технологии. Исследования в области виртуализации и облаков	
	Тематика практических занятий и лабораторных работ	**2**
	Изучение примеров виртуальных машин	
Раздел 2. Безопасность операционных систем		**10**
Тема 2.1. Принципы построения защиты информации в операционных системах	**Содержание**	**4**
	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Порядок обеспечения безопасности информации при эксплуатации операционных систем. Штатные средства ОС для защиты информации.	

	Аутентификация, авторизация, аудит.	
	Тематика практических занятий и лабораторных работ	**6**
	Управление учетными записями пользователей и доступом к ресурсам	
	Изучение средств защиты файлов	
Раздел 3. Особенности работы в современных операционных системах		**20**
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	**Содержание**	**6**
	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX.	
	Операционные системы семейства Mac OS: особенности, преимущества и недостатки.	
	Архитектура Android. Приложения Android	
	Тематика практических занятий и лабораторных работ	**4**
	Источники установки и установка Linux.	
	Работа в ОС Linux.	
Тема 3.2. Операционная система Windows	**Содержание**	**2**
	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	
	Тематика практических занятий и лабораторных работ	**2**
	Первичная настройка Windows.	
Тема 3.3. Серверные операционные системы	**Содержание**	**2**
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	
	Тематика практических занятий и лабораторных работ	**4**
	Работа с сетевой файловой системой	
Итоговое занятие		**2**
Тематика самостоятельной работы при изучении МДК.01.01 1. Создание виртуальной машины. 2. Установка операционной системы. 3. Анализ журнала аудита ОС на рабочем месте. 4. Изучение аналитических обзоров в области построения систем безопасности операционных систем.		**16**
Промежуточная аттестация по МДК.01.01 в форме экзамена		

МДК.01.02 Базы данных		**96**
Раздел 1. Основы теории баз данных		**14**
Тема 1.1. Основные понятия теории баз данных. Модели данных	**Содержание**	**6**
	Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования.	
	Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных.	
	Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	
Тема 1.2. Основы реляционной алгебры	**Содержание**	**2**
	Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями, дополненные Дейтом.	
	Тематика практических занятий и лабораторных работ	**2**
	Операции над отношениями	
Тема 1.3. Базовые понятия и классификация систем управления базами данных	**Содержание**	**2**
	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	
Тема 1.4. Целостность данных как ключевое понятие баз данных	**Содержание**	**2**
	Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	
Раздел 2. Проектирование баз данных		**10**
Тема 2.1. Информационные модели реляционных	**Содержание**	**2**
	Типы информационных моделей. Логические модели данных. Физические модели данных.	
	Тематика практических занятий и лабораторных работ	**2**

баз данных	Проектирование инфологической модели данных	
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	**Содержание**	**2**
	Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам. Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.	
	Тематика практических занятий и лабораторных работ	**2**
	Проектирование структуры базы данных	
	Применение процесса нормализации	
Тема 2.3. Средства автоматизации проектирования	**Содержание**	**2**
	CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	
Раздел 3. Организация баз данных		**14**
Тема 3.1. Создание базы данных. Манипулирование данными.	**Содержание**	**4**
	Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.	
	Тематика практических занятий и лабораторных работ	**2**
	Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	**Содержание**	**2**
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	
	Тематика практических занятий и лабораторных работ	**6**
	Создание взаимосвязей	
	Сортировка, поиск и фильтрация данных, Способы объединения таблиц	
Раздел 4. Управление базой данных с помощью SQL		**14**
Тема 4.1.	**Содержание**	**2**

Структурированный язык запросов SQL	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	
	Тематика практических занятий и лабораторных работ	**2**
	Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL	
Тема 4.2. Операторы и функции языка SQL	**Содержание**	**6**
	Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	
	Тематика практических занятий и лабораторных работ	**4**
	Создание и использование запросов. Группировка и агрегирование данных, коррелированные вложенные запросы	
	Создание в запросах вычисляемых полей. Использование условий	
Раздел 5. Организация распределённых баз данных		**22**
Тема 5.1. Архитектуры распределенных баз данных	**Содержание**	**4**
	Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных.	
	Отличия и преимущества удаленных баз данных от локальных баз данных. Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.	
	Тематика практических занятий и лабораторных работ	**4**
	Управление доступом к объектам базы данных	
Тема 5.2. Серверная часть распределенной базы данных	**Содержание**	**2**
	Планирование и развёртывание СУБД для работы с клиентскими приложениями	
Тема 5.3. Клиентская часть распределенной базы данных	**Содержание**	**6**
	Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация.	

	Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа.	
	Оптимизация производительности работы СУБД.	
	Тематика практических занятий и лабораторных работ	**6**
	Создание форм и отчетов	
	Создание меню. Генерация, запуск.	
Раздел 6. Администрирование и безопасность		
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	**Содержание**	**4**
	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.	
	Тематика практических занятий и лабораторных работ	**2**
	Разработка хранимых процедур и триггеров	
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	**Содержание**	**2**
	Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	
Тема 6.3. Механизмы защиты информации в системах управления базами данных	**Содержание**	**4**
	Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД.	
	Средства защиты информации в базах данных	
	Тематика практических занятий и лабораторных работ	**2**
	Управление правами доступа к базам данных	
Тема 6.4. Копирование	**Содержание**	**2**

и перенос данных. Восстановление данных	Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных	
	Тематика практических занятий и лабораторных работ	**4**
	Аудит данных с помощью средств СУБД и триггеров	
	Резервное копирование и восстановление баз данных	
Тематика самостоятельной работы при изучении МДК.01.02 1. Выполнение индивидуального задания по теме «Проектирование инфологической модели базы данных». 2. Выполнение индивидуального задания по теме «Нормализация отношений». 3. Подготовка рефератов на тему «Развитие СУБД» (конкретной СУБД). 4. Выполнение индивидуального задания по теме «Создание базы данных. Создание таблиц. Организация межтабличных связей» 5. Выполнение индивидуального задания по теме «Организация запросов». 6. Выполнение индивидуального задания по теме «Создание пользовательского приложения средствами СУБД». 7. Разбор синтаксиса хранимых процедур и триггеров. 8. Подготовка рефератов по теме «Организация и использование механизмов защиты базы данных».		**20**
Промежуточная аттестация по МДК.01.02 в форме дифференцированного зачета		**2**
Виды самостоятельных работ при изучении раздела 1 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.		
Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении		**368**
МДК.01.03 Сети и системы передачи информации		**68**
Раздел 1. Теория телекоммуникационных сетей		**36**
Тема 1.1. Основные понятия и определения	**Содержание**	**4**
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	
Тема 1.2. Принципы	**Содержание**	**2**

передачи информации в сетях и системах связи	Назначение и принципы организации сетей. Классификация сетей. Топология сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	
Тема 1.3. Типовые каналы передачи и их характеристики	**Содержание**	**4**
	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	
	Тематика практических занятий и лабораторных работ	**2**
	Расчет пропускной способности канала связи	
Тема 1.4. Кодирование информации в компьютерных сетях	**Содержание**	**4**
	Аналоговое кодирование данных: особенности; виды модуляции. Цифровое кодирование данных: особенности; виды кодов; выбор способа кодирования	
	Помехоустойчивые коды для обнаружения ошибок в сети: разновидности; характеристики; алгоритмы формирования	
	Тематика практических занятий и лабораторных работ	**10**
	Кодирование информации	
	Применение алгоритмов формирования помехоустойчивых кодов	
Тема 1.5.Пакеты передачи информации	**Содержание**	**2**
	Особенности пакетной передачи данных. Назначение и типы информационных пакетов. Структура пакета. Адресация пакетов. Методы взаимодействия. Многоуровневая система вложения пакетов	
Тема 1.6. Аппаратные компоненты компьютерных сетей	**Содержание**	**2**
	Пассивное оборудование компьютерной сети. Активное оборудование компьютерных сетей	
	Тематика практических занятий и лабораторных работ	**6**
	Сетевое оборудование	
	Расчет производительности сети	
Промежуточная аттестация по МДК.01.03 в форме дифференцированного зачета		**2**
Раздел 2. Сети передачи данных		**30**
Тема 2.1. Архитектура и принципы работы	**Содержание**	**6**
	Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по	

современных сетей передачи данных	системам сети и адресация пакетов.	
	Маршрутизация и управление потоками в сетях связи.	
	Протоколы и интерфейсы управления каналами и сетью передачи данных.	
	Тематика практических занятий и лабораторных работ	**8**
	Конфигурирование рабочих станция локальной сети	
Тема 2.2. Беспроводные системы передачи данных	**Содержание**	**2**
	Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	
	Тематика практических занятий и лабораторных работ	**4**
	Настройка Wi-Fi маршрутизатора	
Тема 2.3. Сотовые и спутниковые системы	**Содержание**	**2**
	Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.	
Тема 2.4.Принципы работыв сети	**Содержание**	**4**
	Совместное использование ресурсов сети. Иерархическая структура и атрибуты информационных ресурсов	
	Использование аппаратных ресурсов	
Тема 2.5 Администрирование сети	**Содержание**	**4**
	Создание и изменение учётных записей пользователей, смена паролей. Обслуживание сетевого оборудования	
	Обеспечение комфортной работы удалённых пользователей. Журналы системного протоколирования	
Тематика самостоятельной работы при изучении МДК.01.03 1. Настройка Wi-Fi маршрутизатора 2. Изучение сетевых утилит 3. Конфигурирование сетевого интерфейса 4. Маршрутизация и управление потоками в сетях связи		**14**
Промежуточная аттестация по МДК.01.03 в форме экзамена		
МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**96**
Раздел 1. Разработка защищенных автоматизированных (информационных) систем		

Тема 1.1. Основы информационных систем как объекта защиты.	**Содержание**	**6**
	Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.	
	Основные особенности современных проектов АИС. Электронный документооборот.	
	Тематика практических занятий и лабораторных работ	**2**
	Примеры функционирования автоматизированных информационных систем	
Тема 1.2. Жизненный цикл автоматизированных систем	**Содержание**	**6**
	Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.	
	Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.	
	Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.	
	Тематика практических занятий и лабораторных работ	**2**
	Разработка технического задания на проектирование автоматизированной системы	
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	**Содержание**	**4**
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации	
	Понятие уязвимости угрозы. Классификация уязвимостей.	
	Тематика практических занятий и лабораторных работ	**6**
	Анализ угроз безопасности информации	
	Построение модели угроз	

Тема 1.4. Основные меры защиты информации в автоматизированных системах	**Содержание**	**4**
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	
	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	**Содержание**	**10**
	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	
	Ограничение программной среды. Защита машинных носителей информации	
	Регистрация событий безопасности	
	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	
	Обнаружение (предотвращение) вторжений	
	Контроль (анализ) защищенности информации Обеспечение целостности информационной системы и информации Обеспечение доступности информации	
	Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.	
	Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных	
	Резервное копирование и восстановление данных.	
	Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	
Тема 1.6. Защита	**Содержание**	**2**

информации в распределенных автоматизированных системах	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	
Тема 1.7. Особенности разработки информационных систем персональных данных	**Содержание**	**2**
	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	
	Тематика практических занятий и лабораторных работ	**2**
	Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	
Раздел 2.Эксплуатация защищенных автоматизированных систем.		**46**
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	**Содержание**	**6**
	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	
	Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	
	Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	
Тема 2.2. Администрирование автоматизированных систем	**Содержание**	**2**
	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных	**Содержание**	**2**
	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	

(информационных) систем в защищенном исполнении		
Тема 2.4. Защита от несанкционированного доступа к информации	**Содержание**	**6**
	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.	
	Классификация автоматизированных систем. Требования по защите информации от НСД для АС	
	Требования защищенности СВТ от НСД к информации	
	Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	
Промежуточная аттестация по МДК.01.04 в форме дифференцированного зачета		**2**
Тема 2.5. Средства защиты информации от несанкционированного доступа	**Содержание**	**6**
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.	
	Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.	
	Обеспечение целостности информационной системы и информации	
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	**Содержание**	**4**
	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	
	Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	
	Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном	

	исполнении	
	Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	
	Тематика практических занятий и лабораторных работ	**6**
	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	
Тема 2.7. Документация на защищаемую автоматизированную систему	**Содержание**	**2**
	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	
	Тематика практических занятий и лабораторных работ	**12**
	Оформление основных эксплуатационных документов на автоматизированную систему.	
Тематика самостоятельной работы при изучении МДК.01.04 1. Разработка концепции защиты автоматизированной (информационной) системы 2. Анализ банка данных угроз безопасности информации 3. Анализ журнала аудита ОС на рабочем месте 4. Построение сводной матрицы угроз автоматизированной (информационной) системы 5. Анализ политик безопасности информационного объекта 6. Изучение аналитических обзоров в области построения систем безопасности 7. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации		**22**
Промежуточная аттестация по МДК.01.04 в форме дифференцированного зачета		**2**
МДК.01.05. Эксплуатация компьютерных сетей		**138**
Раздел 1. Основы передачи данных в компьютерных сетях		**30**
Тема 1.1. Модели сетевого взаимодействия	**Содержание**	**2**
	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.	

	Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	
Тема 1.2. Физический уровень модели OSI	**Содержание**	**2**
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.	
	Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.	
	Оптоволоконные линии связи	
	Стандарты кабелей. Электрическая проводка.	
	Беспроводная среда передачи.	
	Тематика практических занятий и лабораторных работ	**2**
	Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	
Тема 1.3. Топология компьютерных сетей	**Содержание**	**2**
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.	
	Тематика практических занятий и лабораторных работ	**6**
	Топологии компьютерных сетей	
	Построение сети	
	Построение одноранговой сети	
Тема 1.4. Технологии Ethernet	**Содержание**	**2**
	Обзор технологий построения локальных сетей.	
	Технология Ethernet. Физический уровень.	
	Технология Ethernet. Канальный уровень	
	Тематика практических занятий и лабораторных работ	**2**
	Изучение адресации канального уровня. MAC-адреса.	
Тема 1.5. Технологии коммутации	**Содержание**	**2**
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI.	
	Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	
	Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети	
	Технология PoweroverEthernet	
Тема 1.6. Сетевой	**Содержание**	**2**

протокол IPv4	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.	
	Маршрутизация пакетов IPv4	
	Протоколы динамической маршрутизации	
	Тематика практических занятий и лабораторных работ	**4**
	Преобразование форматов IP-адресов	
	Адресация в IP-сетях	
Тема 1.7. Скоростные и беспроводные сети	**Содержание**	**2**
	Сеть FDDI. Сеть 100VG-AnyLAN Сверхвысокоскоростные сети Беспроводные сети	
	Тематика практических занятий и лабораторных работ	**2**
	Настройка беспроводного сетевого оборудования	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet		**72**
Тема 2.1. Основы коммутации	**Содержание**	**2**
	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах.	
	Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов	
	Тематика практических занятий и лабораторных работ	**2**
	Работа с основными командами коммутатора.	
Тема 2.2. Начальная настройка коммутатора	**Содержание**	**2**
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.	
	Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.	
	Тематика практических занятий и лабораторных работ	**4**
	Команды обновления программного обеспечения коммутатора и	

	сохранения/восстановления конфигурационных файлов	
	Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	
Тема 2.3. Виртуальные локальные сети (VLAN)	**Содержание**	**2**
	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.	
	Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation	
	Тематика практических занятий и лабораторных работ	**6**
	Настройка VLAN на основе стандарта IEEE 802.1Q	
	Настройка протокола GVRP.	
	Настройка сегментации трафика без использования VLAN	
	Настройка функции Q-in-Q (Double VLAN).	
	Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.	
Тема 2.4. Функции повышения надежности и производительности	**Содержание**	**2**
	Протокол Spanning Tree Protocol (STP). Уязвимостипротокола STP.	
	Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.	
	Дополнительные функции защиты от петель. Агрегирование каналов связи.	
	Тематика практических занятий и лабораторных работ	**4**
	Настройка протоколов связующего дерева STP, RSTP, MSTP.	
	Настройка функции защиты от образования петель LoopBackDetection	
	Агрегирование каналов.	
Тема 2.5. Адресация сетевого уровня и маршрутизация	**Содержание**	**2**
	Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.	
	Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.	
	Планирование подсетей IPv6. Протокол NDP.	
	Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.	

	Тематика практических занятий и лабораторных работ	**6**
	Основные конфигурации маршрутизатора.	
	Расширенные конфигурации маршрутизатора.	
	Работа с протоколом CDP.	
	Работа с протоколом TELNET. Работа с протоколом TFTP.	
	Работа с протоколом RIP.	
	Работа с протоколом OSPF.	
	Конфигурирование функции маршрутизатора NAT/PAT.	
	Конфигурирование PPP и CHAP.	
Промежуточная аттестация по МДК.01.05 в форме дифференцированного зачета		**2**
Тема 2.6. Качество обслуживания (QoS)	**Содержание**	**4**
	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	
	Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.	
	Тематика практических занятий и лабораторных работ	**4**
	Настройка QoS. Приоритизация трафика. Управление полосой пропускания	
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	**Содержание**	**4**
	Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.	
	Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.	
	Тематика практических занятий и лабораторных работ	**8**
	Списки управления доступом (AccessControlList)	
	Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.	
	Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	
Тема 2.8. Многоадресная рассылка	**Содержание**	**4**
	Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.	
	Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping).Функция IGMP FastLeave.	
	Тематика практических занятий и лабораторных работ	**6**

	Отслеживание трафика многоадресной рассылки.	
	Отслеживание трафика Multicast	
Тема 2.9. Функции управления коммутаторами	**Содержание**	**4**
	Управление множеством коммутаторов. Протокол SNMP.	
	RMON (Remote Monitoring). Функция Port Mirroring.	
	Тематика практических занятий и лабораторных работ	**6**
	Функции анализа сетевого трафика.	
	Настройка протокола управления топологией сети LLDP.	
Раздел 3. Межсетевые экраны		**32**
Тема 3.1. Основные принципы создания надежнойи безопасной ИТ-инфраструктуры	**Содержание**	**4**
	Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.	
	Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.	
Тема 3.2. Межсетевые экраны	**Содержание**	**4**
	Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.	
	Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.	
	Тематика практических занятий и лабораторных работ	**12**
	Основы администрирования межсетевого экрана	
	Соединение двух локальных сетей межсетевыми экранами	
	Создание политики без проверки состояния.	
	Создание политик для традиционного (или исходящего) NAT.	
	Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing	
Тема 3.3. Системы обнаружения и предотвращения	**Содержание**	**4**
	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.	

проникновений	Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.	
	Тематика практических занятий и лабораторных работ	**4**
	Обнаружение и предотвращение вторжений.	
Тема 3.4. Приоритезация трафика и создание альтернативных маршрутов	**Содержание**	**2**
	Создание альтернативных маршрутов доступа в интернет. Приоритезация трафика.	
	Тематика практических занятий и лабораторных работ	**2**
	Создание альтернативных маршрутов с использованием статической маршрутизации	
Тематика самостоятельной работы при изучении МДК.01.05 1. Физическое кодирование с использованием манчестерского кода 2. Логическое кодирование с использованием скремблирования 3. Подключение клиента к беспроводной сети в инфраструктурном режиме 4. Оценка беспроводной линии связи 5. Проектирования беспроводной сети 6. Сбор информации о клиентских устройствах 7. Планирование производительности и зоны действия беспроводной сети 8. Предпроектное обследование места установки беспроводной сети 9. Обеспечение отказоустойчивости в беспроводных сетях 10. Режимы работы и организация питания точек доступа 11. Сегментация беспроводной сети 12. Настройка QoS 13. Постпроектное обследование и тестирование сети 14. Создание ACL-списка 15. Наблюдение за трафиком в сети VLAN 16. Определение уязвимых мест сети 17. Реализация функций обеспечения безопасности порта коммутатора 18. Исследование трафика 19. Создание структуры сети организации		**30**

20. Определение технических требований 21. Мониторинг производительности сети 22. Создание диаграммы логической сети 23. Подготовка к обследованию объекта 24. Обследование зоны беспроводной связи 25. Формулировка общих целей проекта 26. Разработка требований к сети 27. Анализ существующей сети 28. Определение характеристик сетевых приложений 29. Анализ сетевого трафика 30. Определение приоритетности трафика 31. Изучение качества обслуживания сети 32. Исследование влияния видеотрафика на сеть 33. Определение потоков трафика, построение диаграмм потоков трафика 34. Применение проектных ограничений 35. Определение проектных стратегий для достижения масштабируемости 36. Определение стратегий повышения доступности 37. Определение требований к обеспечению безопасности 38. Разработка ACL-списков для реализации наборов правил межсетевого экрана 39. Использование CIDR для обеспечения объединения маршрутов 40. Определение схемы IP-адресации 41. Определение количества IP-сетей 42. Создание таблицы для выделения адресов 43. Составление схемы сети 44. Анализ плана тестирования и выполнение теста 45. Создание плана тестирования для сети комплекса зданий 46. Проектирование виртуальных частных сетей 47. Безопасная передача данных в беспроводных сетях	
Промежуточная аттестация по МДК.01.05 в форме дифференцированного зачета	**2**

Виды самостоятельных работ при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.	
Производственная практика **Виды работ:** 1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения 3. Настройка программного обеспечения с соблюдением требований по защите информации 4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам 5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением 6. Настройка встроенных средств защиты информации программного обеспечения 7. Проверка функционирования встроенных средств защиты информации программного обеспечения 8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения 9. Обслуживание средств защиты информации в компьютерных системах и сетях 10. Обслуживание систем защиты информации в автоматизированных системах 11. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем 12. Проверка работоспособности системы защиты информации автоматизированной системы 13. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации 14. Контроль стабильности характеристик системы защиты информации автоматизированной системы 15. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем 16. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	**162**
Экзамен по профессиональному модулю (экзамен квалификационный)	
Всего	***738***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы дисциплины требует наличия учебных кабинетов: компьютерного класса, лаборатории технологий обеспечения информационной безопасности и защищенных информационных систем;

Оборудование компьютерного класса:

- посадочные места по количеству обучающихся;
- доска для написания мелом;
- рабочее место преподавателя;
- проектор
- переносной экран;

Оборудование лаборатории:

- посадочные места с персональными компьютерами и сетевым оборудованием по количеству обучающихся;
- доска для написания маркером
- проектор
- экран настенный
- программно-аппаратные комплексы ФПСУ-IP
- спектральный анализатор с набором антенн
- шумомер с октавными фильтрами
- нановольтметр
- аппаратно-программные средства управления доступом к данным
- средства дублирования и восстановления данных
- средства мониторинга состояния автоматизированных систем
- источники бесперебойного и аварийного питания
- охранная и пожарная сигнализация
- специализированное оборудование по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок
- технические средства контроля эффективности защиты информации от утечки по акустическому каналу
- технические средства контроля эффективности защиты информации от утечки по каналу побочных электромагнитных излучений и наводок
- средства сканирования защищенности компьютерных сетей
- устройства чтения смарт-карт и радиометок

3.2. Информационное обеспечение обучения

3.2.1. Основные источники

1 Староверова, Н. А. Операционные системы : учебник / Н. А. Староверова. — Санкт-Петербург : Лань, 2019. — 308 с. — ISBN 978-5-8114-4000-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125737

2 Гостев, И. М. Операционные системы : учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453469

3 Операционные системы. Программное обеспечение : учебник / составитель Т. П. Куль. — Санкт-Петербург : Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131045

4 Кумскова, И.А. Базы данных : учебник / Кумскова И.А. — Москва : КноРус, 2020. — 400 с. — ISBN 978-5-406-07467-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://book.ru/book/932493

5 Волк, В. К. Базы данных. Проектирование, программирование, управление и администрирование : учебник / В. К. Волк. — Санкт-Петербург : Лань, 2020. — 244 с. — ISBN 978-5-8114-4189-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126933

6 Нестеров, С. А. Базы данных : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2020. — 230 с. — (Профессиональное образование). — ISBN 978-5-534-11629-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457142

7 Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456638

8 Кутузов, О. И. Инфокоммуникационные системы и сети : учебник / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — Санкт-Петербург : Лань, 2020. — 244 с. — ISBN 978-5-8114-4546-2. — Текст : электронный // Лань : электронно-библиотечная систем— URL: https://e.lanbook.com/book/136177

9 Зараменских, Е. П. Информационные системы: управление жизненным циклом : учебник и практикум для среднего профессионального образования / Е. П. Зараменских. — Москва : Издательство Юрайт, 2020. — 431 с. — (Профессиональное образование). — ISBN 978-5-534-11624-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457148

10 Кучуганов, В. Н. Информационные системы: методы и средства поддержки принятия решений : учебное пособие / В. Н. Кучуганов, А. В. Кучуганов. — Москва : Ай Пи Ар Медиа, 2020. — 247 с. — ISBN 978-5-4497-0530-3. — Текст : электронный //

Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97179.html

11 Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — Санкт-Петербург : Лань, 2020. — 392 с. — ISBN 978-5-8114-5342-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147334

12 Журавлев, А. Е. Инфокоммуникационные системы. Программное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — Санкт-Петербург : Лань, 2020. — 376 с. — ISBN 978-5-8114-5343-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147335

13 Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453

3.2.2. Дополнительные источники:

1 Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский. — Санкт-Петербург : Лань, 2020. — 120 с. — ISBN 978-5-8114-4192-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126937

2 Операционные системы. Программное обеспечение : учебник / составитель Т. П. Куль. — Санкт-Петербург : Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131045

3 Назаров, С. В. Современные операционные системы : учебное пособие / С. В. Назаров, А. И. Широков. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 351 с. — ISBN 978-5-4497-0385-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89474.html

4 Назаров, С.В. Операционные системы. Практикум : учебное пособие / Назаров С.В., Гудыно Л.П., Кириченко А.А. — Москва : КноРус, 2020. — 372 с. — ISBN 978-5-406-07707-8. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/933567

5 Гордеев, С. И. Организация баз данных в 2 ч. Часть 1 : учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 310 с. — (Профессиональное образование). — ISBN 978-5-534-11626-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457145

6 Гордеев, С. И. Организация баз данных в 2 ч. Часть 2 : учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 513 с. — (Профессиональное образование). — ISBN 978-5-534-11625-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457146

7 Нестеров, С. А. Базы данных : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2020. — 230 с. — (Профессиональное образование). — ISBN 978-5-534-11629-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457142

8 Советов, Б. Я. Базы данных : учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 420 с. — (Профессиональное образование). — ISBN 978-5-534-09324-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453635

9 Гребешков, А. Ю. Вычислительная техника, сети и телекоммуникации : учебное пособие / А. Ю. Гребешков. — Москва : Горячая линия-Телеком, 2017. — 190 с. — ISBN 978-5-9912-0492-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111047

10 Крук, Б. И. Телекоммуникационные системы и сети : учебное пособие : в 3 томах. Том 1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под редакцией В. П. Шувалова. — 4-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2018. — 620 с. — ISBN 978-5-9912-0208-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111070

11 Пуговкин, А. В. Основы построения инфокоммуникационных сетей и систем : учебное пособие для вузов / А. В. Пуговкин, Д. А. Покаместов, Я. В. Крюков. — 2-е изд., перераб. и доп. — Санкт-Петербург : Лань, 2020. — 176 с. — ISBN 978-5-8114-5905-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156402

12 Будылдина, Н. В. Сетевые технологии высокоскоростной передачи данных : учебное пособие / Н. В. Будылдина, В. П. Шувалов ; под редакцией В. П. Шувалова. — Москва : Горячая линия-Телеком, 2018. — 342 с. — ISBN 978-5-9912-0536-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111025

13 Гагарина, Л. Г. Разработка и эксплуатация автоматизированных информационных систем : учебное пособие для среднего профобразования / Л. Г. Гагарина, Д. В. Киселев, Е. Л. Федотова ; под ред. Л. Г. Гагариной. -Москва : Форум : Инфра-М, 2007, 2009. - 384 с. : ил.- (Профессиональное образование) . - ISBN 978-5-8199-0316-2. -ISBN 978-5-16-003008-1

14 Симоненко, И. В. Основы технического обслуживания телекоммуникационных систем связи и автоматизации : учебное пособие / И. В. Симоненко, О. В. Петров, В. С. Озарчук. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2020. — 62 с. — ISBN 978-5-7422-6875-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/99826.html

15 Попов, А.А. Эргономика пользовательских интерфейсов в информационных системах : учебное пособие пособие для среднего профобразования / Попов А.А. — Москва : КноРус, 2020. — 304 с. — ISBN 978-5-406-07634-7. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/935936

16 Исаев, Г.Н. Управление информационными системами : учебное пособие / Исаев Г.Н., Роганов А.А. — Москва : КноРус, 2020. — 346 с. — ISBN 978-5-406-07674-3. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/935943

17 Тенгайкин, Е. А. Организация сетевого администрирования. Сетевые операционные системы, серверы, службы и протоколы. Практические работы : учебное пособие / Е. А. Тенгайкин. — Санкт-Петербург : Лань, 2020. — 100 с. — ISBN 978-5-8114-4763-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139326

18 Оливер, Ибе Компьютерные сети и службы удаленного доступа / Ибе Оливер ; перевод И. В. Синицын. — 2-е изд. — Саратов : Профобразование, 2019. — 335 с. — ISBN 978-5-4488-0054-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87999.html

19 Сергеев, А. Н. Основы локальных компьютерных сетей : учебное пособие для вузов / А. Н. Сергеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-6475-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147339

20 Ершова, Н. Ю. Организация вычислительных систем : учебное пособие / Н. Ю. Ершова, А. В. Соловьев. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 221 с. — ISBN 978-5-4497-0904-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102024.html

3.2.3. Периодические издания:

1 Системный администратор : [журнал]. - Москва, 2020

2 Программирование : научный журнал / учредители : ФГБОУ ВО МГУ им. М.В.Ломоносова, РАН, Отделение информатики, вычислительной техники и автоматизации РАН. - Москва : Наука, 2020 - . - ISSN 0132-3474. - Текст : электронный // НЭБ eLibrary [сайт]. — URL: https://www.elibrary.ru/title_about_new.asp?id=7966

3 Информационно-управляющие системы : научный журнал / учредитель : ООО «Информационно[управляющие системы». - Санкт-Петербург : Изд-во Санкт-Петербургского государственного университета аэрокосмического приборостроения, 2020 - . - ISSN 1684-8853. - Текст : электронный // НЭБ eLibrary [сайт]. — URL: https://www.elibrary.ru/title_about.asp?id=25785

3.2.4. Интернет-ресурсы:

1 ЭБС Юрайт. - Интернет- ссылка https://urait.ru/

2 ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/

3 ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/

4 ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/

5 НЭБ eLibrary. - Интернет-ссылка https://www.elibrary.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

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

Минобрнауки России
ФГБОУ ВО «Тульский государственный университет»
Технический колледж им. С.И. Мосина

УТВЕРЖДАЮ
Заместитель директора колледжа
по учебной работе

_____ **Д.А.Матвеева**
«21» января 2021 г.

РАБОЧАЯ ПРОГРАММА

профессионального модуля

ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

для специальности

10.02.05 Обеспечение информационной безопасности

автоматизированных систем

2021

РАССМОТРЕНА

цикловой комиссией информационных технологий

Протокол от «14» января 2021 № 6

Председатель цикловой комиссии _____ И.В. Миляева

СОДЕРЖАНИЕ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

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

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	**Защита информации в автоматизированных системах программными и программно-аппаратными средствами**
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
ПК 2.7.	Разрабатывать проектные решения защиты информации на объекте программно-аппаратными средствами

1.1.2. Общие компетенции

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

ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 12.	Способен применять проектный подход в профессиональной деятельности

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– установки, настройки программных средств защиты информации в автоматизированной системе; – обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; – применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; – учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе.
уметь	– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; – применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

знать	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 794 часов, из них

на освоение МДК – 324 часа,

на самостоятельную работу – 74 часа,

на промежуточную аттестацию – 54 часа

на практики – 342 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 2.1 – ПК 2.7 ОК 1 - ОК 10, ОК 12	**Раздел 1 модуля.** Применение программных и программно-аппаратных средств защиты информации	**222**	**180**	48	30	–	–	**42**
ПК 2.4 ОК 1-ОК 10	**Раздел 2 модуля.** Применение криптографических средств защиты информации	**284**	**144**	56	–	**108**	–	**32**
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	**234**					**234**	–
	Промежуточная аттестация		–	–	–	–	–	–
	По МДК 02.01. дифференцированный зачет в 3 4 семестрах, экзамен в 5 семестре	18						
	По МДК 02.02. дифференцированный зачет в 3 семестре, экзамен в 4 семестре	18						
	Экзамен по профессиональному модулю (экзамен квалификационный) в 6 семестре	18	-	–	–	–	–	–
	Всего:	**794**	**324**	104	30	**108**	**234**	**74**

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации		**240**
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**180**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		**42**
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**	**6**
	Предмет и задачи программно-аппаратной защиты информации	
	Основные понятия программно-аппаратной защиты информации	
	Классификация методов и средств программно-аппаратной защиты информации	
Тема 1.2. Стандарты безопасности	**Содержание**	**4**
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
	Тематика практических занятий и лабораторных работ	**6**
	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. .	
	Работа с содержанием нормативных правовых актов	
	Обзор стандартов. Работа с содержанием стандартов	

Тема 1.3. Защищенная автоматизированная система	**Содержание**	**6**
	Автоматизация процесса обработки информации	
	Понятие автоматизированной системы.	
	Особенности автоматизированных систем в защищенном исполнении.	
	Основные виды АС в защищенном исполнении.	
	Методы создания безопасных систем	
	Методология проектирования гарантированно защищенных КС	
	Дискреционные модели	
	Мандатные модели	
	Тематика практических занятий и лабораторных работ	**4**
	Учет, обработка, хранение и передача информации в АИС	
	Ограничение доступа на вход в систему.	
	Идентификация и аутентификация пользователей	
	Разграничение доступа.	
	Регистрация событий (аудит).	
	Контроль целостности данных	
	Уничтожение остаточной информации.	
	Управление политикой безопасности. Шаблоны безопасности	
	Криптографическая защита. Обзор программ шифрования данных	
	Управление политикой безопасности. Шаблоны безопасности	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**	**4**
	Источники дестабилизирующего воздействия на объекты защиты	
	Способы воздействия на информацию	
	Причины и условия дестабилизирующего воздействия на информацию	
	Тематика практических занятий и лабораторных работ	**2**
	Распределение каналов в соответствии с источниками воздействия на информацию	
Тема 1.5. Принципы программно-аппаратной	**Содержание**	**6**
	Понятие несанкционированного доступа к информации	

защиты информации от несанкционированного доступа	Основные подходы к защите информации от НСД	
	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	
	Доступ к данным со стороны процесса	
	Особенности защиты данных от изменения. Шифрование. Знакомство с системой Криптон. КРИПТОН Шифрование	
	Тематика практических занятий и лабораторных работ	**4**
	Организация доступа к файлам. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД.	
	КРИПТОН Шифрование	
Раздел 2. Защита автономных автоматизированных систем		**48**
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание**	**6**
	Работа автономной АС в защищенном режиме	
	Алгоритм загрузки ОС. Штатные средства замыкания среды	
	Расширение BIOS как средство замыкания программной среды	
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	
Тема 2.2.Защита программ от изучения	**Содержание**	**6**
	Изучение и обратное проектирование ПО	
	Способы изучения ПО: статическое и динамическое изучение	
	Задачи защиты от изучения и способы их решения	
	Защита от отладки.	
	Защита от дизассемблирования	
	Защита от трассировки по прерываниям.	
Тема 2.3. Вредоносное программное обеспечение	**Содержание**	**6**
	Вредоносное программное обеспечение как особый вид разрушающих воздействий	
	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	

	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	
	Бот-неты. Принцип функционирования. Методы обнаружения	
	Классификация антивирусных средств. Сигнатурный и эвристический анализ	
	Защита от вирусов в "ручном режиме"	
	Основные концепции построения систем антивирусной защиты на предприятии	
	Тематика практических занятий и лабораторных работ	**2**
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	
Промежуточная аттестация по МДК.02.01 в форме дифференцированного зачета		**2**
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**	**4**
	Несанкционированное копирование программ как тип НСД	
	Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.	
	Привязка ПО к аппаратному окружению и носителям.	
	Защитные механизмы в современном программном обеспечении	
	Тематика практических занятий и лабораторных работ	**2**
	Защита информации от несанкционированного копирования с использованием специализированных программных средств	
	Защитные механизмы в приложениях	
Тема 2.5. Защита информации на машинных носителях	**Содержание**	**6**
	Проблема защиты отчуждаемых компонентов ПЭВМ.	
	Методы защиты информации на отчуждаемых носителях. Шифрование.	
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	
	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	
	Безвозвратное удаление данных. Принципы и алгоритмы.	
	Тематика практических занятий и лабораторных работ	**4**

	Применение средства восстановления остаточной информации на примере Foremost или аналога	
	Применение специализированного программного средства для восстановления удаленных файлов	
	Применение программ для безвозвратного удаления данных	
	Применение программ для шифрования данных на съемных носителях	
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**	**4**
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	
	Устройства Touch Memory	
	Тематика практических занятий и лабораторных работ	**4**
	Crypton rutocen для Windows 2000/XP	
	Crypton Lock	
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**	**4**
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	
	Использование сетевых снифферов в качестве СОВ	
	Аппаратный компонент СОВ	
	Программный компонент СОВ	
	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
Раздел 3. Защита информации в локальных сетях		**12**
Тема 3.1. Основы построения защищенных сетей	**Содержание**	**6**
	Сети, работающие по технологии коммутации пакетов	
	Стек протоколов TCP/IP. Особенности маршрутизации.	
	Штатные средства защиты информации стека протоколов TCP/IP.	
	Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	
	Знакомство с системой Криптон	
Тема 3.2. Средства организации VPN	**Содержание**	**4**
	Виртуальная частная сеть. Функции, назначение, принцип построения	
	Криптографические и некриптографические средства организации VPN	

	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	
	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Тематика практических занятий и лабораторных работ	**2**
	Развертывание VPN	
Раздел 4. Защита информации в сетях общего доступа		**10**
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание**	**8**
	Методы защиты информации при работе в сетях общего доступа.	
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности	
	Основные типы firewall. Симметричные и несимметричные firewall.	
	Уровень 1. Пакетные фильтры	
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	
	Уровень 3. Proxy-сервера прикладного уровня	
	Однохостовые и мультихостовые firewall.	
	Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций	
	Требования по сертификации межсетевых экранов	
	Тематика практических занятий и лабораторных работ	**2**
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	
	Изучение различных способов закрытия "опасных" портов	
Раздел 5. Защита информации в базах данных		**12**
Тема 5.1. Защита информации в базах данных	**Содержание**	**8**
	Основные типы угроз. Модель нарушителя	
	Средства идентификации и аутентификации. Управление доступом	
	Средства контроля целостности информации в базах данных	
	Средства аудита и контроля безопасности. Критерии защищенности баз данных	
	Применение криптографических средств защиты информации в базах данных	
	Тематика практических занятий и лабораторных работ	**4**
	Изучение штатных средств защиты СУБД MS SQLServer	

	Crypton ArcMail	
Промежуточная аттестация по МДК.02.01 в форме дифференцированного зачета		**2**
Раздел 6. Мониторинг систем защиты		**22**
Тема 6.1. Мониторинг систем защиты	**Содержание**	**8**
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	
	Классификация отслеживаемых событий. Особенности построения систем мониторинга	
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	
	Классификация сетевых мониторов	
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
	Тематика практических занятий и лабораторных работ	**2**
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**	**2**
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	
	Тематика практических занятий и лабораторных работ	**2**
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Тематика практических занятий и лабораторных работ**	**8**
	Эмулятор функций шифрования УКЗД «Криптон» Часть 1	
	Эмулятор функций шифрования УКЗД «Криптон» Часть 2	
	Crypton Word	
	Crypton Excel	
Курсовая работа		**30**

Тематика курсовых работ 1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах 6. Защита сред виртуализации 7. Средства обеспечения информационной безопасности банков данных. 8. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.	
Тематика самостоятельной работы при изучении МДК.02.01 1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты	**42**
Промежуточная аттестация по МДК.02.01 в форме экзамена	**18**
Виды самостоятельных работ при изучении раздела 1 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.	
Раздел 2 модуля. Применение криптографических средств защиты информации	**284**
МДК.02.02. Криптографические средства защиты информации	**144**

Введение	**Содержание**	**2**
	Предмет и задачи криптографии. История криптографии. Основные термины	
Раздел 1. Математические основы защиты информации		**34**
Тема 1.1. Математические основы криптографии	**Содержание**	**30**
	Элементы теории множеств. Понятие алгебраической операции и ее свойства: понятие группоида, полугруппы, группы.	
	Кольца, поля	
	Делимость чисел. Признаки делимости. Простые и составные числа.	
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	
	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	
	Китайская теорема об остатках.	
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	Арифметические операции над большими числами.	
	Эллиптические кривые и их приложения в криптографии.	
	Тематика практических занятий и лабораторных работ	**4**
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	
	Решение сравнений. Решение задач с элементами теории чисел.	
Раздел 2. Классическая криптография		**36**
Тема 2.1. Методы криптографического защиты информации	**Содержание**	**8**
	Классификация основных методов криптографической защиты. Методы симметричного шифрования	
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	

	Методы перестановки. Табличная перестановка, маршрутная перестановка	
	Методы гаммирования. Гаммирование с конечной и бесконечной гаммами	
	Тематика практических занятий и лабораторных работ	**6**
	Применение классических шифров замены	
	Применение классических шифров перестановки	
	Применение метода гаммирования	
Тема 2.2. Криптоанализ	**Содержание**	**6**
	Основные методы криптоанализа. Криптографические атаки.	
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	
	Перспективные направления криптоанализа, квантовыйкриптоанализ.	
	Тематика практических занятий и лабораторных работ	**6**
	Криптоанализ шифра простой замены методом анализа частотности символов	
	Криптоанализ классических шифров методом полного перебора ключей	
	Криптоанализ шифра Вижинера	
	Криптоанализ магического квадрата и квадрата Полибия	
	Криптоанализ шифра Тримериуса	
Промежуточная аттестация по МДК.02.02 в форме дифференцированного зачета		**2**
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	**4**
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	Тематика практических занятий и лабораторных работ	**6**
	Применение методов генерации ПСЧ	
Раздел 3. Современная криптография		**68**
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	**6**
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	
	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств.	

	Изучение современных программных и аппаратных криптографических средств	
	Тематика практических занятий и лабораторных работ	**4**
	Кодирование информации по Хэммингу	
	Кодирование информации по Хаффману	
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**	**4**
	Общие сведения. Структурная схема симметричных криптографических систем	
	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	
	Тематика практических занятий и лабораторных работ	**6**
	Операции сложения и циклического сдвига. Алгоритм RC4	
	Изучение программной реализации алгоритмов Магма и Кузнечик	
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	**4**
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	
	Элементы теории чисел в криптографии с открытым ключом.	
	Тематика практических занятий и лабораторных работ	**4**
	Реализации асимметричного алгоритма RSA	
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**	**4**
	Аутентификация данных. Общие понятия. ЭП. МАС. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Тематика практических занятий и лабораторных работ	**6**
	Применение различных функций хеширования, анализ особенностей хешей	
	Изучение программно-аппаратных средств Криптон, реализующих основные функции ЭП	
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	**4**
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	
	Тематика практических занятий и лабораторных работ	**6**

	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
	Применение протокола Эль-Гамаля для обмена ключами шифрования.	
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**	**4**
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**	**4**
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	Тематика практических занятий и лабораторных работ	**4**
	Применение аутентификации по одноразовым паролям.	
	Реализация алгоритмов создания одноразовых паролей	
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**	**4**
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
	Тематика практических занятий и лабораторных работ	**4**
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	
	Реализация простейших стеганографических алгоритмов	
Итоговое занятие		**2**
Тематика самостоятельной работы при изучении МДК.02.02 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров.		**32**

4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии	
Промежуточная аттестация по МДК.02.02 в форме экзамена	**18**
Виды самостоятельной работы при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	
Учебная практика раздела 2 модуля **Виды работ:** Написание алгоритма, программная реализация: – Методов замены: одноалфавитная замена, многоалфавитные подстановки, пропорциональные шифры, метод гаммирования. – Методов перестановки: перестановка с фиксированным периодом d, перестановка по таблице. – Блочные шифры с закрытым ключом: использование операций в блочных алгоритмах симметричного шифрования, сеть Фейштеля, агоритмы шифрования и расшифрования DES, алгоритм криптографического преобразования данных ГОСТ 28147-89. – Поточные шифры и генераторы псевдослучайных чисел: поточные шифры, использование генераторов ПСЧ при потоковом шифровании, генераторы ПСЧ на основе сдвиговых регистров с обратной связью, генератор ПСЧ на основе алгоритма BBC, алгоритм RC4. – Алгоритмы шифрования с открытым ключом: алгоритм RSA, алгоритм Диффи-Хеллана, алгоритм Эль-Гамаля	**108**
Производственная практика по ПМ.02	**234**

Виды работ – Анализ принципов построения систем информационной защиты производственных подразделений. – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении – Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	
Экзамен по профессиональному модулю (экзамен квалификационный)	**18**
Всего:	**794**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы требует наличия учебного кабинета информатики, лаборатории программных и программно-аппаратных средств защиты информации и технологий обеспечения информационной безопасности и защищенных информационных систем.

Оборудование учебного кабинета информатики:

- рабочее место преподавателя;
- посадочные места по количеству обучающихся;
- наглядные стенды, схемы, плакаты, слайды.

Оборудование лаборатории программных и программно-аппаратных средств защиты информации:

- общее количество посадочных мест;
- рабочие места с персональными компьютерами и сетевым оборудованием;
- рабочее место преподавателя;
- антивирусные программные комплексы; программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения вторжений;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства выявления уязвимостей в автоматизированных системах и средствах вычислительной техники;
- программные средства криптографической защиты информации;
- комплект демонстрационных стендов.

Оборудование лаборатории технологий обеспечения информационной безопасности и защищенных информационных систем:

- рабочие места с персональными компьютерами и сетевым оборудованием;
- доска для написания маркером; проектор; экран настенный;
- программно-аппаратные комплексы ФПСУ-IP;
- спектральный анализатор с набором антенн;
- комплект, шумомер с октавными фильтрами; нановольтметр;
- аппаратно-программные средства управления доступом к данным;
- средства дублирования и восстановления данных;
- средства мониторинга состояния автоматизированных систем; источники бесперебойного и аварийного питания; охранная и пожарная сигнализация;
- специализированное оборудование по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок;
- технические средства контроля эффективности защиты информации от утечки по акустическому каналу;
- технические средства контроля эффективности защиты информации от утечки по каналу побочных электромагнитных излучений и наводок;
- средства сканирования защищенности компьютерных сетей;
- устройства чтения смарт-карт и радиометок;
- программно-аппаратный комплекс защиты информации, включая криптографические средства защиты информации.

3.2. Информационное обеспечение обучения

3.2.1 Основные источники:

1 Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под редакцией А. В. Душкина. — Москва : Горячая линия-Телеком, 2018. — 248 с. — ISBN 978-5-9912-0470-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111053

2 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548

3 Бабаш, А.В. Криптографические методы защиты информации : учебник / Бабаш А.В., Баранова Е.К. — Москва : КноРус, 2020. — 189 с. — ISBN 978-5-406-00169-1.—— Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://book.ru/book/933943

4 Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450998

5 Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. — ISBN 978-5-4497-0340-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89455.html

3.2.2. Дополнительные печатные источники:

1 Джонс, К. Д. Инструментальные средства обеспечения безопасности : учебное пособие / К. Д. Джонс, М. Шема, Б. С. Джонсон. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 913 с. — ISBN 978-5-4497-0871-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102011.html

2 Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие / С. Н. Никифоров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-6352-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146885

3 Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 431 с. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102070.html

4 Гельбух, С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация : учебное пособие / С. С. Гельбух. — Санкт-Петербург : Лань, 2019. — 208 с. — ISBN 978-5-8114-3474-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118646

5 Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102069.html

6 Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453

7 Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97571.html

8 Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2020. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450277

9 Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450538

10 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

11 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

12 Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

13 Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

14 Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

15 Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

16 Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

17 Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

18 Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

19 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

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

21 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

22 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

47 ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

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

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

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

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

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

53 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

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

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

56 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

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

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

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

3.2.3. Периодические издания:

1 Системный администратор : [журнал]. - Москва, 2020

2 Программирование : научный журнал / учредители : ФГБОУ ВО МГУ им. М.В.Ломоносова, РАН, Отделение информатики, вычислительной техники и автоматизации РАН. - Москва : Наука, 2020 - . - ISSN 0132-3474. - Текст : электронный // НЭБ eLibrary [сайт]. — URL: https://www.elibrary.ru/title_about_new.asp?id=7966

3 Информационно-управляющие системы : научный журнал / учредитель : ООО «Информационно[управляющие системы». - Санкт-Петербург : Изд-во Санкт-Петербургского государственного университета аэрокосмического приборостроения, 2020 - . - ISSN 1684-8853. - Текст : электронный // НЭБ eLibrary [сайт]. — URL: https://www.elibrary.ru/title_about.asp?id=25785

3.2.4. Интернет-ресурсы:

1. ЭБС Юрайт. - Интернет- ссылка https://urait.ru/
2. ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/
3. ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/
4. ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/
5. НЭБ eLibrary. - Интернет-ссылка https://www.elibrary.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике, защита курсовой работы
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных)	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием	

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	
ПК 2.7. Разрабатывать проектные решения защиты информации на объекте программно-аппаратными средствами	Демонстрация алгоритма проведения проектных работ по защите информации на объекте программно-аппаратными средствами	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный Защита проекта
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Демонстрация ответственности за принятые решения, обоснованность самоанализа и коррекция результатов собственной работы	

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
физической подготовленности.		
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	Эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	
ОК 12. Способен применять проектный подход в профессиональной деятельности	Эффективность организация работы в решении профессиональных задач	

Минобрнауки России
ФГБОУ ВО «Тульский государственный университет»
Технический колледж им. С.И. Мосина

УТВЕРЖДАЮ
Заместитель директора колледжа
по учебной работе

_____ **Д.А.Матвеева**
«21» января 20 21 г.

РАБОЧАЯ ПРОГРАММА

профессионального модуля

ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ
для специальности

10.02.05 Обеспечение информационной безопасности

автоматизированных систем

2021

РАССМОТРЕНА

цикловой комиссией информационных технологий

Протокол от «14» января 2021 № 6

Председатель цикловой комиссии _____И.В. Миляева

Составитель: Симаков А.Ю., преподаватель, канд. хим. наук

СОДЕРЖАНИЕ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

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

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	**Защита информации техническими средствами**
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.
ПК 3.6.	Применять биометрические системы безопасности
ПК 3.7.	Разрабатывать проектные решения защиты информации на объекте техническими средствами

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 12.	Способен применять проектный подход в профессиональной деятельности.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.
уметь	– применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации
знать	– порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

	– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 760 часов, из них

на освоение МДК – 388 часов,

на самостоятельную работу 84 часа,

на промежуточную аттестацию – 54 часа

на практики – 234 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 3.1- ПК.3.4 ОК 1– ОК10	**Раздел 1 модуля.** Применение технической защиты информации	**176**	**144**	66	–	–	–	**32**
ПК 3.5 ОК 01–ОК10	**Раздел 2 модуля.** Применение инженерно-технических средств физической защиты объектов информатизации	**176**	**144**	70	30		–	**32**
ПК 3.6 ОК 01–ОК10	**Раздел 3 модуля.** Применение биометрических систем безопасности	**120**	**100**	20				**20**
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	**234**					**234**	–
	Промежуточная аттестация							
	По МДК 03.01. дифференцированный зачет в 3 семестре, экзамен в 4 семестре	**18**						
	По МДК 03.02. дифференцированный зачет в 4 семестре, экзамен в 5 семестре	**18**						
	По МДК 03.03. дифференцированный зачет в 5 семестре							
	Экзамен по профессиональному модулю (экзамен квалификационный) в 6 семестре	**18**						
	Всего:	**760**	**388**	156	30		**234**	**84**

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение технической защиты информации		**194**
МДК.03.01 Техническая защита информации		**144**
Раздел 1. Концепция инженерно-технической защиты информации		**6**
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**2**
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**4**
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	
Раздел 2. Теоретические основы инженерно-технической защиты информации		**24**
Тема 2.1. Информация как предмет защиты	**Содержание**	**4**
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	Тематика практических занятий и лабораторных работ	**4**
	Содержательный анализ основных руководящих, нормативных и методических документов по	

	защите информации и противодействию технической разведке.	
Тема 2.2. Технические каналы утечки информации	**Содержание**	**4**
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	
	Тематика практических занятий и лабораторных работ	**4**
	Видовые, сигнальные и вещественные демаскирующие признаки	
	Способы записи информации на различные виды носителей. Виды модуляции (манипуляции) сигналов	
Тема 2.3. Методы и средства технической разведки	**Содержание**	**4**
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Тематика практических занятий и лабораторных работ	**4**
	Условия разведывательного контакта	
	Доступ к источникам информации без физического проникновения в контролируемую зону	
Раздел 3. Физические основы технической защиты информации		**16**
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**6**
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика практических занятий и лабораторных работ	**4**
	Измерение параметров физических полей	
Тема 3.2. Физические процессы при	**Содержание**	**2**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических	

подавлении опасных сигналов	преобразований. Экранирование. Зашумление.	
	Тематика практических занятий и лабораторных работ	**4**
	Генерирование помех	
Раздел 4. Системы защиты от утечки информации		**60**
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**4**
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**4**
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Защита от утечки по проводному каналу	
Промежуточная аттестация по МДК.03.01 в форме дифференцированного зачета		**2**
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**4**
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**6**
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от	

	несанкционированной утечки по электромагнитному каналу.	
	Тематика практических занятий и лабораторных работ	**6**
	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**6**
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Защита от утечки по телефонному каналу	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**4**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Защита информации по электросетевому каналу	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**4**
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Тематика практических занятий и лабораторных работ	**2**
	Защиты информации по оптическому каналу	
Раздел 5. Применение и эксплуатация технических средств защиты информации		**34**
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**8**
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты	

	информации.	
	Тематика практических занятий и лабораторных работ	**6**
	Определение параметров фоновых шумов и физических полей	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**8**
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
	Тематика практических занятий и лабораторных работ	**12**
	Установка и настройка технических средств защиты информации	
Итоговое занятие		**2**
Тематика самостоятельной работы при изучении МДК.03.01 1. Средства защиты акустической информации. 2. Виброакустические средства современных систем обеспечения информационной безопасности. 3. Средства защиты от ПЭМИН, современное состояние, проблемы и решения. 4. Средства обеспечения информационной безопасности проводных сетей общего доступа.		**32**
Промежуточная аттестация по МДК.03.01 в форме экзамена		**18**
Виды самостоятельной работы при изучении раздела 1 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		**194**
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**144**
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		**24**
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**6**
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и	

	способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	
	Тематика практических занятий и лабораторных работ	**2**
	Определение категории объектов информатизации	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**6**
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Тематика практических занятий и лабораторных работ	**10**
	Построения интегрированных систем охраны объектов.	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		**56**
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**6**
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Тематика практических занятий и лабораторных работ	**10**
	Монтаж датчиков пожарной и охранной сигнализации	
Тема 2.2. Система контроля и управления доступом	**Содержание**	**8**
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	
	Тематика практических занятий и лабораторных работ	**6**
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	

	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**4**
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
Промежуточная аттестация по МДК.03.02 в форме дифференцированного зачета		**2**
	Тематика практических занятий и лабораторных работ	**6**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**4**
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	
	Тематика практических занятий и лабораторных работ	**4**
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема 2.5 Система воздействия	**Содержание**	**2**
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	
	Тематика практических занятий и лабораторных работ	**6**
	Анализ показателей технических средств воздействия и применение технических средств воздействия.	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		**30**
Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание**	**6**
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	
	Тематика практических занятий и лабораторных работ	**10**
	Проектирование установки системы пожарно-охранной сигнализации	

	Рассмотрение принципов работы системы видеонаблюдения и ее проектирование	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**2**
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	
	Тематика практических занятий и лабораторных работ	**12**
	Диагностика системы пожарно-охранной сигнализации	
	Диагностика системы видеонаблюдения	
Итоговое занятие		**2**
Курсовой проект (работа)		**30**
Тематика курсового проекта (работы) 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества. 4. Инструментальные средства анализа рисков информационной безопасности. 5. Сертификация и аудит объекта информатизации: организационные аспекты 6. Методика проведения аудита объекта информатизации. Этапы проведения аудита 7. Варианты аудита безопасности объекта информатизации. 8. Методы тестирования системы защиты объекта информатизации 9. Средства анализа защищенности объекта информатизации		
Тематика самостоятельной работы при изучении МДК.03.02 – Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. – Размещение периметровых средств обнаружения на местности. – Самостоятельное изучения порядка допуска субъектов на охраняемые объекты.		**32**
Промежуточная аттестация по МДК.03.02 в форме экзамена		**18**
Виды самостоятельной работы при изучении раздела 2 модуля		

Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите. Работа над курсовой работой: планирование выполнения курсовой работы, определение задач работы, изучение литературных источников, проведение предпроектного исследования …		
Раздел 3 модуля. Применение биометрических систем безопасности		**120**
МДК.03.03. Биометрические системы безопасности		**100**
Тема 1.Общие сведения о биометрических системах безопасности	**Содержание**	**14**
	Научно-технический прогресс и история развития средств биометрической идентификации и аутентификации	
	Классификация биометрических методов идентификации; основные термины биометрии	
	Статические и динамические методы биометрической аутентификации	
	Характеристики биометрических методов и систем	
	Расчет числовых характеристик точности биометрических методов	
	Структура биометрической системы безопасности	
	Ознакомительный обзор биометрических систем безопасности	
Тема 2. Методы и аппаратура для распознавания человека по изображению лица	**Содержание**	**26**
	Основные преимущества использования фотопортрета для идентификации	
	Метод геометрических характеристик лица	
	Реализация метода геометрических характеристик	
	Метод главных компонент	
	Реализация метода главных компонент	
	Метод эластичных графов	
	Метод анализа видеопотока	
	Интеллектуальные методы распознавания лица	
	Основные преимущества использования фотопортрета для идентификации	
	Метод геометрических характеристик лица	
	Структура и свойства нейронных сетей	
	Методы построения трехмерных компьютерных моделей лица	

	Построение трехмерной модели объекта	
	Биологические основы контактной и дистантной термометрии	
	Физические принципы и аппаратура для получения термограмм;	
	Методы фильтрации и обработки термограмм	
	Тематика практических занятий и лабораторных работ	**4**
	Знакомство с программой распознавания по методу геометрических характеристик	
	Знакомство с программой распознавания по методу главных компонент	
Тема 3. Методы и аппаратура для распознавания человека по форме руки и отпечаткам пальцев	**Содержание**	**10**
	Преимущества использования формы руки для распознавания человека; устройства HandKey и их применение	
	Биологические основы папиллярного рисунка кожи человека.	
	Преимущества использования отпечатков пальцев для распознавания личности	
	Методы и аппаратура для получения отпечатков пальцев	
	Автоматизированные системы криминально-дактилоскопического учета и регистрации	
	Тематика практических занятий и лабораторных работ	**6**
	Изучение методов распознавания изображения папиллярного узора пальцев	
	Изучение структуры и состава систем дактилоскопического учета	
	Изучение сканера отпечатков пальцев	
Тема 4.Методы распознавания человека по индивидуальным признакам глаз	**Содержание**	**8**
	Строение глаза и основные сложности в получении его изображений	
	Математические методы решения задачи выделения биометрических характеристик; получение модели изображения радужной оболочки глаза	
	Аппаратура для сканирования радужной оболочки	
	Преимущества использования сетчатки глаза как объекта для аутентификации человека и основные сложности в получении её изображения	
	Тематика практических занятий и лабораторных работ	**4**
	Изучение систем распознавания личности по радужной оболочке глаза	
	Построение математической модели радужной оболочки глаза	
Тема 5. Динамические методы	**Содержание**	**8**
	Физические и фонетические основы речи	

биометрической аутентификации	Вопросы распознавания речи и распознавания человека по её параметрам	
	Перспективы использования систем фонографического учета	
	Распознавание человека по двигательным динамическим параметрам	
	Тематика практических занятий и лабораторных работ	**2**
	Анализ фонограмм речи для аутентификации дикторов	
Тема 6. Технические, правовые и культурные аспекты применения биометрических технологий	**Содержание**	**12**
	Основные задачи интегрированной системы безопасности и место биометрических технологий в их решении	
	Структура интегрированной системы безопасности	
	Опрос с использованием полиграфа	
	Технологии и научное обоснование опроса с использованием полиграфа	
	Законодательство РФ и других стран о применении биометрических технологий;	
	Перспективы использования биометрических систем безопасности	
	Тематика практических занятий и лабораторных работ	**4**
	Изучение интегрированных систем безопасности предприятий, применяющих биометрические методы	
	Морально-этические аспекты использования биометрических технологий	
Промежуточная аттестация по МДК.03.03 в форме дифференцированного зачета		**2**
Тематика самостоятельной работы при изучении МДК.03.03 – Биометрические характеристики человека. – Методы и аппаратура для распознавания человека по ДНК – Методы и аппаратура для распознавания человека по подписи – Методы и аппаратура для распознавания человека по клавиатурному почерку – Устройства управления и исполнения биометрических средств защиты.		
Виды самостоятельной работы при изучении раздела 3 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		
Производственная практика профессионального модуля **Виды работ** 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации;		**234**

2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения, биометрических систем; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	
Экзамен по профессиональному модулю (экзамен квалификационный)	***18***
Всего	***760***

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы требует наличия учебного кабинета информационной безопасности, лаборатории технических средств защиты информации и технологий обеспечения информационной безопасности и защищенных информационных систем

Оборудование учебного кабинета информационной безопасности:

- рабочее место преподавателя;
- посадочные места по количеству обучающихся;
- рабочие места с персональными компьютерами и сетевым оборудованием;
- мультимедиапроектор, экран, интерактивная доска, программное обеспечение, оргсредства, комплект демонстрационных стендов.

Оборудование лаборатории технических средств защиты информации:

- посадочные места по количеству обучающихся;
- рабочие места с персональными компьютерами и сетевым оборудованием, подключенными к локальной вычислительной сети и информационно-телекоммуникационной сети «Интернет»;
- рабочее место преподавателя;
- средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок (индикатор поля – частотомер
- скоростной поисковый приемник;
- устройства защиты телефонных переговорови слаботочных линий;
- устройства защиты сотовой связи;
- генератор акустического шума;
- средства измерения параметров физических полей;
- стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
- информационная доска для маркера;
- комплект демонстрационных стендов;
- программное обеспечение.

Оборудование лаборатории технологий обеспечения информационной безопасности и защищенных информационных систем:

- рабочие места с персональными компьютерами и сетевым оборудованием;
- доска для написания маркером;
- проектор;
- экран настенный;
- программно-аппаратные комплексы ФПСУ-IP;
- спектральный анализатор с набором антенн;
- комплект, шумомер с октавными фильтрами;

– нановольтметр;
– аппаратно-программные средства управления доступом к данным;
– средства дублирования и восстановления данных;
– средства мониторинга состояния автоматизированных систем;
– источники бесперебойного и аварийного питания;
– охранная и пожарная сигнализация;
– специализированное оборудование по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок;
– технические средства контроля эффективности защиты информации от утечки по акустическому каналу;
– технические средства контроля эффективности защиты информации от утечки по каналу побочных электромагнитных излучений и наводок;
– средства сканирования защищенности компьютерных сетей;
– устройства чтения смарт-карт и радиометок;
– программно-аппаратный комплекс защиты информации, включая криптографические средства защиты информации.

3.2. Информационное обеспечение обучения

3.2.1. Основные источники:

1 Мельников, В.П. Информационная безопасность : учебник для среднего профессионального образования / Мельников В.П., Куприянов А.И. — Москва : КноРус, 2018. — 267 с. — ISBN 978-5-406-05072-9.-Текст : электронный // ЭБС Юрайт [сайт]. — — URL: https://book.ru/book/924214;

2 Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356 ;

3 Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89451.html ;

4 Бурькова, Е. В. Физическая защита объектов информатизации : учебное пособие / Е. В. Бурькова. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2017. — 158 с. — ISBN 978-5-7410-1697-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/71349.html;

5 Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057;

6 Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0334-7. — Текст :

электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89449.html ;

1.2.2. Дополнительные источники:

1 Гельбух, С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация : учебное пособие / С. С. Гельбух. — Санкт-Петербург : Лань, 2019. — 208 с. — ISBN 978-5-8114-3474-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118646;

2 Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102069.html;

3 ГОСТ Р 52633-2006.Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. Введ.2007-04-01. М. : Стандартинформ, 2007. IV,20с. : ил. (Защита информации) .

4 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

6 Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

7 Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

8 Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

9 Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

10 Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

11 Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

12 Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

13 Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

14 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

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

16 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

17 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

50 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

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

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

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

3.2.3. Периодические издания:

1. Системный администратор : [журнал]. - Москва, 2020

2. Программирование : научный журнал / учредители : ФГБОУ ВО МГУ им. М.В.Ломоносова, РАН, Отделение информатики, вычислительной техники и автоматизации РАН. - Москва : Наука, 2020 - . - ISSN 0132-3474. - Текст : электронный // НЭБ eLibrary [сайт]. — URL: https://www.elibrary.ru/title_about_new.asp?id=7966

3. Информационно-управляющие системы : научный журнал / учредитель : ООО «Информационно[управляющие системы». - Санкт-Петербург : Изд-во Санкт-Петербургского государственного университета аэрокосмического приборостроения, 2020 - . - ISSN 1684-8853. - Текст : электронный // НЭБ eLibrary [сайт]. — URL: https://www.elibrary.ru/title_about.asp?id=25785

3.2.4 Интернет-ресурсы:

1. ЭБС Юрайт. - Интернет- ссылка https://urait.ru/
2. ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/
3. ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/
4. ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/
5. НЭБ eLibrary. - Интернет-ссылка https://www.elibrary.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	
ПК 3.6 Применять биометрические системы безопасности	Проявлять умения в применении биометрических систем безопасности	
ПК 3.7 Разрабатывать проектные решения защиты информации на объекте техническими средствами	Демонстрация алгоритма проведения проектных работ по защите информации на объекте техническими средствами	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный Защита проекта
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Демонстрация ответственности за принятые решения, обоснованность самоанализа и коррекция результатов собственной работы	

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Грамотность устной и письменной речи, ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик	

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
необходимого уровня физической подготовленности.		
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	Эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	
ОК 12. Способен применять проектный подход в профессиональной деятельности	Эффективность организация работы в решении профессиональных задач	

Минобрнауки России
ФГБОУ ВО «Тульский государственный университет»
Технический колледж им. С.И. Мосина

УТВЕРЖДАЮ
Заместитель директора колледжа
по учебной работе

_____ **Д.А.Матвеева**
«21» января 2021 г.

РАБОЧАЯ ПРОГРАММА

профессионального модуля

ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ

для специальности

10.02.05 Обеспечение информационной безопасности

автоматизированных систем

2021

РАССМОТРЕНА

цикловой комиссией информационных технологий

Протокол от «14» января 2021 № 6

Председатель цикловой комиссии _____И.В. Миляева

Составитель: Груднов М.В., мастер производственного обучения
Техического колледжа им. С.И. Мосина ТулГУ

СОДЕРЖАНИЕ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

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

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

1.1.2. Общие компетенции:

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

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– выполнения требований техники безопасности при работе с вычислительной техникой; – организации рабочего места оператора электронно-вычислительных и вычислительных машин; – подготовки оборудования компьютерной системы к работе; – инсталяции, настройки и обслуживания программного обеспечения компьютерной системы; – управления файлами; – применения офисного программного обеспечения в соответствии с прикладной задачей; – использования ресурсов локальной вычислительной сети; – использования ресурсов, технологий и сервисов Интернет; – создания Web-приложений; – применения средств защиты информации в компьютерной системе, – выполнять электромонтажные работы.
уметь	– выполнять требования техники безопасности при работе с вычислительной техникой; – производить подключение блоков персонального компьютера и периферийных устройств; – производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; – диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; – выполнять инсталляцию системного и прикладного программного обеспечения; – создавать и управлять содержимым документов с помощью текстовых процессоров; – создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; – создавать и управлять содержимым презентаций с помощью редакторов презентаций; – использовать мультимедиа проектор для демонстрации презентаций; – вводить, редактировать и удалять записи в базе данных; – эффективно пользоваться запросами базы данных; – создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; – производить сканирование документов и их распознавание; – производить распечатку, копирование и тиражирование документов на принтере и других устройствах; – управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; – осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера;

	– создавать Web-приложения; – осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; – осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; – осуществлять резервное копирование и восстановление данных – читать и составлять электрические схемы; – выполнять несложные операции по электромонтажу.
знать	– требования техники безопасности при работе с вычислительной техникой; – основные принципы устройства и работы компьютерных систем и периферийных устройств; – классификацию и назначение компьютерных сетей; – виды носителей информации; – программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета; – основы разработки Web-приложений; – основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы; – инструменты, приспособления, оборудование и материалы для выполнения работ по электромонтажу; – способы и примеры работы при выполнении операции по электромонтажу; – организацию рабочего места и уход за ним.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 162 часов, из них
на практики – 162 часов

2СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 4.1 – ПК 4.4 ОК1–ОК 10	**Раздел 1 модуля**. Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»	**162**	–	–	–	**162**	–	–
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	–					–	–
	Экзамен квалификационный по присвоению по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»			–	–	–	–	–
	Всего:	**162**	**-**	–	–	**162**	–	–

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся	Объем часов
1	2	3
Раздел модуля 1. Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»		**162**
УП.04. Учебная практика		**162**
Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения		**24**
Тема 1.1. Работа с устройствами компьютерной системы	**Тематика практических занятий и лабораторных работ**	**8**
	Соблюдение техники безопасности при работе на ЭВМ Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка Установка и замена расходных материалов для принтеров, ксерокса, плоттера.	
Тема 1.2. Работа с программным обеспечением компьютерной системы	**Тематика практических занятий и лабораторных работ**	**8**
	Установка операционной среды, настройка интерфейса ОС (рабочий стол, безопасность системы, подключение к сети). Установка прикладных программ. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете	
Тема 1.3. Диагностика неисправностей системы, ведение документации	**Тематика практических занятий и лабораторных работ**	**8**
	Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ	
Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и		**56**

содержанием баз данных, работа в графических редакторах		
Тема 2.1. Работа в текстовом процессоре	Сканирование текстовых документов и их распознавание Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов Форматирование и редактирование документов в текстовом процессоре. Работа с таблицами в текстовом процессоре. Работа с диаграммами в текстовом процессоре. Работа с графическими объектами в текстовом процессоре. Печать документов в текстовом процессоре.	**16**
Тема 2.2. Работа в редакторе электронных таблиц	**Тематика практических занятий и лабораторных работ** Создание и форматирование таблицы в редакторе электронных таблиц Вычисление с помощью формул в электронной таблице Работа со встроенными функциями в электронной таблице Работа со списками в электронной таблице Создание форм для ввода данных в таблицы Создание и работа с диаграммами и графиками Обмен данными между текстовым процессором и электронной таблицей	**16**
Тема 2.3. Работа в программе подготовки и просмотра презентаций	**Тематика практических занятий и лабораторных работ** Построение презентации различными способами Обработка объектов слайдов презентации Настройка анимации объектов Настройка показа и демонстрация результатов работы средствами мультимедиа	**8**
Тема 2.4. Работа в системе управления базами данных	**Тематика практических занятий и лабораторных работ** Ввод данных в таблицы базы данных Создание простых запросов без параметров и с параметрами. Создание отчетов.	**8**
Тема 2.5.	**Тематика практических занятий и лабораторных работ**	**8**

Работа в графических редакторах	Рисование объектов средствами графического редактора. Работа с заливками и контурами в программе векторной графики. Работа с текстом в программе векторной графики. Работа с эффектами программе векторной графики. Вставка и редактирование готового изображения с использованием программ растровой графики. Работа с цветом с использованием программ растрой графики. Работа со слоями с использованием программ растрой графики. Работа со спецэффектами с использованием программ растровой графики.	
Раздел 3. Использование ресурсов технологий и сервисов Интернета		**30**
Тема 3.1. Работа с ресурсами Интернета	**Тематика практических занятий и лабораторных работ**	**8**
	Создание и обмен письмами электронной почты. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера. Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов. Пересылка и публикация файлов данных в Интернете.	
Тема 3.2. Основы разработки Web- и мультимедиа-приложений	Структура HTML-документа. Разметка текста. Работа со ссылками и изображениями. Работа с таблицами и формами. Базовые понятия CSS. Селекторы, каскадность, наследование, приоритеты. Основы JavaScript. Условия, циклы, массивы, функции, объекты. Препроцессор Less	**22**
Раздел 4. Обеспечение защиты информации в компьютерной системе		**8**
Тема 4.1. Защита информации при работе с офисными приложениями	**Тематика практических занятий и лабораторных работ**	**8**
	Использование штатных средств защиты операционной системы и прикладных программ. Применение парольной защиты. Установка антивирусных программ, их настройка. Обновление базы. Выполнение архивирования данных. Выполнение резервного копирования и восстановления данных	
Раздел 5. Электромонтажная практика		**36**
Тема 5.1. Вводное	**Тематика практических занятий и лабораторных работ**	**2**

занятие.	Ознакомление с оборудованием и рабочими местами. Виды электромонтажных работ. Материалы, провода, кабели.	
Тема 5.2. Техника безопасности и пожарная безопасность при электромонтажных работах	**Тематика практических занятий и лабораторных работ**	**2**
	Защитные средства, применяемые при электромонтажных работах. Уровни безопасных напряжений при работе с электрифицированным инструментом. Заземление корпуса инструмента. Виды и причины травматизма при электромонтажных работах. Организация рабочего места.	
Тема 5.3. Организация работ; применяемый инструмент, Материалы, приборы	**Тематика практических занятий и лабораторных работ**	**2**
	Распределение работ, монтажные площадки. Работы на высоте. Получение оборудования, материалов, инструмента. Составление исполнительных схем, протоколов, испытаний, смонтированных устройств. Инструменты, применяемые при производстве электромонтажных работ	
Тема 5.4. Соединение и оконцевание проводов и кабелей	**Тематика практических занятий и лабораторных работ**	**4**
	Требования, предъявляемые к контактным соединениям. Разъемные и неразъемные контактные соединения, их применение. Материалы, инструменты и приспособления, применяемые при соединении, ответвлении и оконцевании проводов. Способы оконцевания проводов и кабелей опрессовкой, пайкой. Особенности выполнения неразрывных соединений медных и алюминиевых проводов. Ответвление проводов. Брак, меры его предупреждения и устранения	
Тема 5.5. Чтение принципиальных и монтажных электрических схем	**Тематика практических занятий и лабораторных работ**	**4**
	Порядок составления электромонтажных схем. Функциональные схемы автоматизации (ФСА). Принципиальные электрические схемы (ПЭС) управления, регулирования, автоблокировки. Схемы внешних электрических проводок. Чертежи направлений трасс электрических и трубных проводок. Чертежи установки средств автоматизации первичных приборов, щитов, пультов	
Тема 5.6. Лужение и пайка	**Тематика практических занятий и лабораторных работ**	**6**
	Назначение пайки, лужения. Пайка мягкими припоями и лужением. Подготовка шва для пайки. Приготовление припоев. Приготовление флюсов. Подготовка к пайке. Пайка электрическими паяльниками. Лужение, пайка твердыми припоями. Отделка мест пайки. Основные виды брака. Применение пайки и лужения в электромонтажных работах. Допустимая температура нагрева спаиваемых изделий. Требования к паяной поверхности, зачистка концов одножильных и многожильных монтажных проводов. Заделка концов для пре-	

	дохранения от распускания с помощью полихлорвиниловых трубок, изоляционной ленты, нитяного бандажа.	
Тема 5.7. Монтаж, демонтаж и пайка полупроводниковых элементов, резисторов, конденсаторов	**Тематика практических занятий и лабораторных работ**	**4**
	Разновидности и типы полупроводниковых элементов, конструктивные особенности диодов и транзисторов. Способы механического крепления полупроводниковых элементов и печатных плат. Проверка исправности полупроводников, измерение их основных параметров. Особенности монтажа, демонтажа и пайки проводников, радиодеталей и микросхем на печатных платах. Предотвращение перегрева полупроводников при пайке. Последовательность операций при выполнении монтажных работ.	
Тема 5.8. Монтаж и демонтаж ламповых панелей, разъемов, переключателей и блоков питания	**Тематика практических занятий и лабораторных работ**	**4**
	Назначение ламповых панелей, требования к ним и их разновидности. Способы механического крепления ламповых панелей на шасси приборов на панелях. Подготовка лепестков к пайке. Способы крепления радиодеталей и проводников на панелях. Переключатели и разъемы, основные типы и их назначение, подготовка к пайке. Способы крепления деталей на панелях. Техническая документация на монтаж блока питания. Последовательность операций при выполнении монтажных работ. Поверка качества монтажа. Испытание блока питания на соответствие заданным параметрам. Техника безопасности при испытании блока питания.	
Тема 5.9. Монтаж электрических соединительных линий	**Тематика практических занятий и лабораторных работ**	**4**
	Назначение и типы электрических соединительных линий. Технические условия монтажа, разметка, установка крепежных изделий. Лотки и короба. Монтаж кабеля по лоткам, полосе, тросу и другим конструкциям. Монтаж электрических линий, выполненных проводом в отдельных трубах. Затяжка проводов в трубы. Устройство герметизированных вводов, смонтированных электрических линий в электрооборудовании. Заполнение форм протоколов. Соединение проводов пайкой и сваркой, болтовыми соединениями, опрессовкой и т.п. Монтаж с подмостков, лестниц, козел. Техника безопасности при монтаже электрических соединительных линий	
Тема 5.10. Монтаж измерительных преобразователей и	**Тематика практических занятий и лабораторных работ**	**4**
	Основные правила и требования по монтажу измерительных преобразователей. Инструменты. Разметка. Методы контроля. Монтаж первичных преобразователей для измерения температуры,	

отборных устройств	давления и вакуума, сужающих устройств для измерения расхода, уровня, концентрации растворов и контроля состава газов. Установка дистанционного контроля температуры, влажности и др. Выбор места установки. Техника безопасности при монтаже первичных преобразователей и отборных устройств.	
Промежуточная аттестация по учебной практике		**2**
Экзамен квалификационный по присвоению по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»		**6**
Всего		**162**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация примерной программы модуля предполагает наличие компьютерного класса, лаборатории информационных технологий и лаборатории информационных технологий, программирования и баз данных

Оборудование компьютерного класса:

- рабочие места с персональными компьютерами и сетевым оборудованием;
- доска для написания мелом;
- проектор;
- переносной экран.

Оборудование лаборатории информационных технологий:

- рабочие места с персональными компьютерами и сетевым оборудованием;
- рабочее место преподавателя;
- программное обеспечение;
- мультимедиапроектор, персональный компьютер, экран, персональные ЭВМ, сетевое оборудование, подключенными к локальной вычислительной сети и информационно-телекоммуникационной сети «Интернет»
- специализированная мебель и оргтехника, демонстрационный материал: наглядные стенды, схемы, плакаты, карты, слайды, видеофильмы, аудиоматериалы, программное обеспечение.

Оснащение лаборатории информационных технологий, программирования и баз данных:

- рабочие места с персональными компьютерами и сетевым оборудованием, подключенные к информационно-коммуникационной сети «Интернет»;
- программное обеспечение;
- информационная доска для маркера;
- принтер;
- комплект демонстрационных стендов.

3.2. Информационное обеспечение реализации программы

3.2.1. Основные источники:

1. Лошаков, С. Периферийные устройства вычислительной техники : учебное пособие / С. Лошаков. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 419 с. — ISBN 978-5-4497-0555-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/94858.html

2. Гаврилов, М. В. Информатика и информационные технологии : учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 383 с. — (Профессиональное образование). — ISBN 978-5-534-03051-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449286

3. Куприянов, Д. В. Информационное обеспечение профессиональной деятельности : учебник и практикум для среднего профессионального образования / Д. В. Куприянов. — Москва : Издательство Юрайт, 2020. — 255 с. — (Профессиональное образование). — ISBN 978-5-534-00973-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451935

3.2.2. Дополнительные источники:

1. Акимова, Е. В. Вычислительная техника : учебное пособие / Е. В. Акимова. — Санкт-Петербург : Лань, 2020. — 68 с. — ISBN 978-5-8114-4925-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/142354

2. Угринович, Н.Д. Информатика. Практикум : учебное пособие для среднего профессионального образования / Угринович Н.Д. — Москва : КноРус, 2020. — 264 с. — ISBN 978-5-406-07320-9. — Текст : электронный // ЭБС Book.ru [сайт]. —URL: https://book.ru/book/932058

3.2.3. Интернет-ресурсы:

1. ЭБС Юрайт. - Интернет- ссылка https://urait.ru/
2. ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/
3. ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/
4. ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/
5. НЭБ eLibrary. - Интернет-ссылка https://www.elibrary.ru/

1. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.		ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 4.4Обеспечивать применение средств защиты информации в компьютерной системе	Применение средств защиты информации в компьютерной системе	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция	

	результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать	- эффективность	

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