Приложение
к программе СПО10.02.05
Обеспечение информационной безопасности
Автоматизированных систем

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

2024г.

СОДЕРЖАНИЕ

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

Цель и планируемые результаты освоения профессионального модуля

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
ВД1	**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.
ПК1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках

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 и компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности
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 других технических средств информатизации.

Количество часов, отводимое на освоение профессионального модуля

Всего часов ___**724**_____

в том числе в форме практической подготовки - 454 часа

Из них на освоение МДК - **460** часов

в том числе самостоятельная работа_____12_____

промежуточная аттестация по МДК _____18_____

практики, в том числе учебная - **108** часов

производственная - **144**часов

Промежуточная аттестация – экзамен по модулю – **12** часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час	В т.ч. в форме практической. подготовки	Объем профессионального модуля, ак. час.							
				Обучение по МДК						Практики	
				Всего	В том числе						
					Теоретическое обучение	Лаборат. и практ. занятий	самостоятельная работа	Консультации	Промежуточная аттестация (экзамен по МДК)	Учебная	Производственная
1	2	3	4	5	6	7	8	9	10	11	12
ПК 1.1. ОК 1, ОК 2, ОК 9	**Раздел 1 модуля.** Установка и настройка автоматизированных (информационных) систем в защищенном исполнении	**172**	80	**172**	86	80	6				
ПК 1.2., ПК 1.3, ПК 1.4 ОК 1, ОК 2, ОК 9	**Раздел 2 модуля.** Администрирование автоматизированных (информационных) систем в защищенном исполнении	**288**	110	**288**	108	142	6	14	18		
	Учебная практика	**108**	108							108	
	Производственная практика, часов	**144**	144								144
	Промежуточная аттестация (экзамен по модулю)	**12**	12								
	Всего:	**724**	454	**724**	194	222	12	14	18	**108**	**144**

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 1модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении		**177**
МДК.01.01Операционные системы		**92**
Раздел1.Элементытеориионационныхсистем. Свойства операционных систем		
Тема 1.1. Основы теории и 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	
	Создание и изучение структуры разделов жесткого диска	
	Операции с файлами	
Тема 1.3.Модульная структура	**Содержание**	**4**
	Экзо ядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме.	

операционных систем, пространство пользователя	Оболочки операционных систем.	
	Тематика практических занятий и лабораторных работ	**4**
	Работа в консольном и графическом режимах	
Тема 1.4.Управление памятью	**Содержание**	**4**
	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	**4**
	Мониторинг за использование памяти	
Тема 1.5.Управление процессами, многопроцессорные системы	**Содержание**	**4**
	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие	
	Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	
	Тематика практических занятий и лабораторных работ	**4**
	Управление процессами»	
	Наблюдение за использованием ресурсов системы	
Тема 1.6. Виртуализация и облачные технологии	**Содержание**	**4**
	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования	
	Облачные технологии. Исследования в области виртуализации облаков	
	Тематика практических занятий и лабораторных работ	**4**
	Изучение примеров виртуальных машин (VMware,VBox)	
Раздел 2. Безопасность операционных систем		
Тема 2.1.Принципы построения защиты информации в операционных	**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.	

системах	Аутентификация, авторизация, аудит.	
	Тематика практических занятий и лабораторных работ	**6**
	Управление учетными записями пользователей и доступом к ресурсам	
	Аудит событий системы	
	Изучение штатных средств защиты информации в операционных системах	
Раздел3. Особенности работы в современных операционных системах		
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	**Содержание**	**6**
	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX.	
	Операционные системы семейства MacOS: особенности, преимущества и недостатки.	
	Архитектура Android. Приложения Android	
	Тематика практических занятий и лабораторных работ	**4**
	Создание дистрибъютива Linux. Установка.	
	Работа в ОСLinux.	
Тема3.2. Операционная система Windows	**Содержание**	**4**
	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-выводв Windows.	
	Тематика практических занятий и лабораторных работ	**2**
	Установка и первичная настройка Windows.	
Тема3.3.Серверные операционные системы	**Содержание**	**2**
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	
	Тематика практических занятий и лабораторных работ	**4**
	Работа с сетевой файловой системой.	
	Работа с серверной ОС, например, AltLinux.	
Примерная тематика самостоятельной работы при изучении МДК.01.01 1. Создание виртуальной машины. 2. Установка операционной системы. 3. Анализ журнал аудита ОС на рабочем месте.		**4**

4.Изучение аналитических обзоров в области построения систем безопасности операционных систем.		
Промежуточная аттестация по МДК. 01.01 дифференцированный зачет		**2**
МДК.01.02 Базы данных		**80**
Раздел 1.Основы теории баз данных		
Тема1.1.Основные понятия теории баз данных. Модели данных	**Содержание**	**2**
	Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования.	
	Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных.	
	Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Коддадля 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	
Тема1.2.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 (по выбору)	
Тема 1.3. 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		
Тема 2.1.	**Содержание**	**2**

Информационные модели реляционных баз данных	Типы информационных моделей. Логические модели данных. Физические модели данных.	
	Тематика практических занятий и лабораторных работ	**2**
	Проектирование инфологической модели данных	
Тема2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	**Содержание**	**2**
	Необходимостьнормализации.Аномалиивставки,удаленияиобновления.Приведениетаблицык первой,второйитретьейнормальнымформам.Дальнейшаянормализациятаблиц.Четвертаяипятая нормальные формы. Применение процесса нормализации.	
	Тематика практических занятий и лабораторных работ	**2**
	Проектирование структуры базы данных	
Тема2.3.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.	
	Тематика практических занятий и лабораторных работ	**2**
	Проектирование базы данных с использованием CASE-средств	
Раздел 3. Организация баз данных		
Тема3.1.Создание базы данных. Манипулирование данными.	**Содержание**	**2**
	Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными.Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.	
	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.	**Содержание**	**4**
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	

Объединение таблиц	**Тематика практических занятий и лабораторных работ**	**4**
	Создание взаимосвязей	
	Сортировка, поиски фильтрация данных	
	Способы объединения таблиц	
Раздел 4. Управление базой данных с помощью SQL		
Тема 4.1. Структурированный язык запросов SQL	**Содержание**	**2**
	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	
	Тематика практических занятий и лабораторных работ	**2**
	Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL	
Тема4.2.Операторыи функции языка SQL	**Содержание**	**2**
	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		
Тема 5.1. Архитектуры распределенных баз данных	**Содержание**	**2**
	Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных.	
	Отличия и преимущества удаленных баз данных от локальных баз данных. Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.	
	Тематика практических занятий и лабораторных работ	**2**
	Управление доступом к объектам базы данных	
Тема 5.2.Серверная	**Содержание**	**2**

часть распределенной базы данных	Планирование и развёртывание СУБД для работы с клиентскими приложениями	
	Тематика практических занятий и лабораторных работ	**2**
	Установка СУБД. Настройка компонентов СУБД.	
Тема5.3. Клиентская часть распределенной базы данных	**Содержание**	**2**
	Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация.	
	Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа.	
	Оптимизация производительности работы СУБД.	
	Тематика практических занятий и лабораторных работ	**6**
	Создание форм и отчетов	
	Создание меню. Генерация, запуск.	
	Профилирование запросов клиентских приложений.	
Раздел 6. Администрирование и безопасность		
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	**Содержание**	**2**
	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.	
	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	**Содержание**	**2**

защиты информации в системах управления базами данных	Средства идентификации 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 и перенос данных. Восстановление данных	**Содержание**	**2**
	Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных	
	Тематика практических занятий и лабораторных работ	**4**
	Аудит данных с помощью средств СУБД и триггеров	
	Резервное копирование и восстановление баз данных	
Примерная тематика самостоятельной работы при изучении МДК.01.02 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».		**2**
Промежуточная аттестация по МДК.01.02 дифференцированный зачет		**2**

Примерные виды самостоятельных работ при изучении раздела 1модуля 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		**288**
МДК. 01.03 Сети и системы передачи информации		**60**
Раздел 1.Теория телекоммуникационных сетей		
Тема 1.1. Основные понятия и определения	**Содержание**	**4**
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	
Тема 1.2. Принципы передачи информации в сетях и системах связи	**Содержание**	**2**
	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	
Тема 1.3. Типовые каналы передачи и их характеристики	**Содержание**	**4**
	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	
	Тематика практических занятий и лабораторных работ	6
	Расчет пропускной способности канала связи	

Раздел 2. Сети передачи данных		
Тема 2.1.Архитектура и принципы работы современных сетей передачи данных	**Содержание**	**4**
	Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи.	
	Протоколы интерфейсы управления каналами и сетью передачи данных.	
	Тематика практических занятий и лабораторных работ	**18**
	Конфигурирование сетевого интерфейса рабочей станции	
	Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP	
	Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне	
	Диагностика и разрешение проблем сетевого уровня	
	Диагностика и разрешение проблем протоколов транспортного уровня	
	Диагностика и разрешение проблем протоколов прикладного уровня	
Тема 2.2. Беспроводные системы передачи данных	**Содержание**	**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	**6**
	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.	
Примернаятематикасамостоятельнойработыприизучении МДК.01.03 1. Настройка Wi-Fi маршрутизатора 2. Изучение сетевых утилит 3. Конфигурирование сетевого интерфейса 4. Маршрутизация и управление потоками в сетях связи		**5**
Консультации		**4**
Промежуточная аттестация по МДК.01.03 (экзамен комплексный)		**3**

МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**104**
Раздел 1. Разработка защищенных автоматизированных (информационных) систем		
Тема 1.1. Основы информационных систем как объекта защиты.	**Содержание**	**4**
	Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологи и 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	**4**
	Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	
Тема 1.2. Жизненный цикл автоматизированных систем	**Содержание**	**4**
	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	**6**
	Разработка технического задания на проектирование автоматизированной системы	
Тема1.3.Угрозы безопасности информации в автоматизированных	**Содержание**	**2**
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации	

системах	Понятие уязвимости угрозы. Классификация уязвимостей.	
	Тематика практических занятий и лабораторных работ	**10**
	Категорирование информационных ресурсов	
	Анализ угроз безопасности информации	
	Построение модели угроз	
Тема1.4.Основные меры защиты информации в автоматизированных системах	**Содержание**	**2**
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	
	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	
Тема1.5.Содержание и порядок эксплуатации АС в защищенном исполнении	**Содержание**	**12**
	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	
	Ограничение программной среды. Защита машинных носителей информации	
	Регистрация событий безопасности	
	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	
	Обнаружение (предотвращение) вторжений	
	Контроль(анализ) защищенности информации Обеспечение целостности информационной системы и информации Обеспечение доступности информации	
	Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.	
	Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных	
	Резервное копирование и восстановление данных.	

	Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	
Тема1.6. Защита информации в распределенных автоматизированных системах	**Содержание**	**2**
	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурныхифункциональныхсхемзащищенныхавтоматизированныхинформационныхсистем.	
Тема1.7.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	**4**
	Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	
Раздел 2. Эксплуатация защищенных автоматизированных систем.		
Тема 2.1.Особенности эксплуатации автоматизированных систем в защищенном исполнении.	**Содержание**	**2**
	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 (информационных) систем в защищенном исполнении	**Содержание**	**2**
	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	
Тема 2.4. Защита от несанкционированного доступа к информации	**Содержание**	**4**
	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.	
	Классификация автоматизированных систем. Требования по защите информации от НСД для АС	
	Требования защищенности СВТ от НСД к информации	
	Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	
Тема 2.5 .СЗИ от НСД	**Содержание**	**4**
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.	
	Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.	
	Обеспечение целостности информационной системы и информации	
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	
	Тематика практических занятий и лабораторных работ	**14**

	Установка и настройка СЗИ от НСД	
	Защита входа в систему (идентификация и аутентификация пользователей)	
	Разграничение доступа к устройствам	
	Управление доступом	
	Использование принтеров для печати конфиденциальных документов. Контроль печати	
	Настройка системы для задач аудита	
	Настройка контроля целостности и замкнутой программной среды	
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	
Тема 2.6. 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 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	**4**
	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	**2**
	Оформление основных эксплуатационных документов на автоматизированную систему.	
Примерная тематика самостоятельной работы при изучении МДК.01.04		**5**

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 политики 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		
Консультации **Промежуточная аттестация по МДК. 01.04 экзамен комплексный**		**4** **3**
МДК. 01.05.Эксплуатация компьютерных сетей		**124**
Раздел1.Основыпередачиданныхвкомпьютерныхсетях		
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.	
	Тематика практических занятий и лабораторных работ	**2**
	Изучение элементов кабельной системы.	
Тема 1.2. Физический уровень модели OSI	**Содержание**	**4**
	Понятие линии 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 не экранированной витой пары (UTP)	
	Сварка оптического волокна	

Тема1.3. Топология компьютерных сетей	**Содержание**	**2**
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий**.**	
	Тематика практических занятий и лабораторных работ	**4**
	Разработка топологии сети небольшого предприятия	
	Построение одноранговой сети	
Тема1.4. 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.	
Тема1.5.Технологии коммутации	**Содержание**	**4**
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутациии модель OSI.	
	Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	
	Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети	
	Технология Powerover Ethernet	
	Тематика практических занятий и лабораторных работ	**2**
	Создание коммутируемой сети	
Тема1.6.Сетевой протокол IPv4	**Содержание**	**4**
	Сетевой уровень. Протокол IPверсии4. Общие функции классовой и бесклассовой адресации. Выделение адресов.	
	Маршрутизация пакетов IPv4	
	Протоколы динамической маршрутизации	
	Тематика практических занятий и лабораторных работ	**2**
	Изучение IP-адресации.	
Тема 1.7.Скоростные	**Содержание**	**2**

и беспроводные сети	Сеть FDDI. Сеть100VG-AnyLAN Сверх высокоскоростные сети. Беспроводные сети	
	Тематика практических занятий и лабораторных работ	**2**
	Настройка беспроводного сетевого оборудования	
Раздел 2.Технологии коммутации и маршрутизации современных сетей Ethernet		
Тема 2.1. Основы коммутации	**Содержание**	**4**
	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах.	
	Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов	
	Тематика практических занятий и лабораторных работ	**2**
	Работа с основными командами коммутатора.	
Тема 2.2. Начальная настройка коммутатора	**Содержание**	**4**
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.	
	Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.	
	Тематика практических занятий и лабораторных работ	**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 IEEE802.1Q. Статические и динамические VLAN. Протокол GVRP.	
	Q-in-QVLAN. VLAN на основе портов и протоколов–стандарт IEEE802.1v. Функция Traffic Segmentation	

	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 DoubleVLAN).	
	Самостоятельная работа по созданию ЛВС на основе стандарта IEEE802.1Q.	
Тема 2.4. Функции повышения надежности и производительности	**Содержание**	**2**
	Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.	
	Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.	
	Дополнительные функции защиты от петель. Агрегирование каналов связи.	
	Тематика практических занятий и лабораторных работ	**4**
	Настройка протоколов связующего дерева STP, RSTP, MSTP.	
	Настройка функции защиты от образования петель Loop Back Detection	
	Агрегирование каналов.	
Тема2.5. Адресация сетевого уровня и маршрутизация	**Содержание**	**4**
	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 протоколомOSPF.	

	Конфигурирование функции маршрутизатора NAT/PAT.	
	Конфигурирование PPP и CHAP.	
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	**2**
	Настройка QoS. Приоритизация трафика. Управление полосой пропускания	
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	**Содержание**	**2**
	Списки управления доступом(ACL).Функции контроля над подключением узлов к портам коммутатора.	
	Аутентификация пользователей 802.1x.802.1xGuestVLAN. Функции защиты ЦПУ коммутатора.	
	Тематика практических занятий и лабораторных работ	**2**
	Списки управления доступом (AccessControlList)	
	Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.	
	Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	
Тема 2.8. Многоадресная рассылка	**Содержание**	**2**
	Адресация многоадресногоIP-рассылки. MAC-адреса групповой рассылки.	
	Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMPSnooping).Функция IGMPFastLeave.	
	Тематика практических занятий и лабораторных работ	**4**
	Отслеживание трафика многоадресной рассылки.	
	Отслеживание трафика Multicast	
Тема 2.9. Функции управления коммутаторами	**Содержание**	**2**
	Управление множеством коммутаторов. Протокол SNMP.	
	RMON (RemoteMonitoring). Функция PortMirroring.	
	Тематика практических занятий и лабораторных работ	**4**
	Функции анализа сетевого трафика.	

	Настройка протокола управления топологией сети LLDP.	
Раздел3.Межсетевые экраны		
Тема3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	**Содержание**	**2**
	Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.	
	Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.	
Тема3.2. Межсетевые экраны	**Содержание**	**2**
	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	**4**
	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	
Тема3.3. Системы обнаружения и предотвращения проникновений	**Содержание**	**2**
	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.	
	Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS.Сильные стороны и ограниченность IDPS.	
	Тематика практических занятий и лабораторных работ	**2**
	Обнаружение и предотвращение вторжений.	
Тема3.4. Приоритизация трафика и создание альтернативных маршрутов	**Содержание**	**2**
	Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.	
	Тематика практических занятий и лабораторных работ	**2**
	Создание альтернативных маршрутов с использованием статической маршрутизации	

Примерная 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	**2**
Консультации	**6**
Промежуточная аттестация по МДК. 01.05 экзамен	**6**

Учебная практика **Виды работ** 1. Установка программного обеспечения в соответствии с технической документацией. 2. Настройка параметров работы программного обеспечения, включая системы управления базами данных. 3. Настройка компонентов подсистем защиты информации операционных систем. 4. Управление учетными записями пользователей. 5. Работа в операционных системах с соблюдением действующих требований по защите информации. 6. Установка обновления программного обеспечения. 7. Контроль целостность подсистем защиты информации операционных систем. 8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных 9. Использование программных средств для архивирования информации. 10. Проведение аудита защищенности автоматизированной системы. 11. Установка, настройка и эксплуатация сетевых операционных систем. 12. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 13. Организация работ с удаленными хранилищами данных и базами данных. 14. Организация защищенной передачи данных в компьютерных сетях. 15. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.	***108***

16. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. 17. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	
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	***144***
Консультации ***Экзамен по модулю***	**6** **6**
Всего	***724***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

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

Оборудование учебного кабинета и рабочих мест кабинета:

- Рабочее место преподавателя;
- Посадочные места для обучающихся;
- Аудиовизуальный комплекс;
- Комплект обучающего материала (комплект презентаций).

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

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

Оборудование лаборатории рабочих мест лаборатории сетей и систем передачи информации:

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

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

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

Информационное обеспечение обучения

Основные печатные источники

1. Заяц, А. М. Организация беспроводных Ad Hoc и Hot Spot сетей в среде ОС Windows: учебное пособие для спо / А. М. Заяц, С. П. Хабаров. — Санкт-Петербург: Лань, 2021— 220 с. — ISBN 978-5-8114-6974-1.

2. Костров Б. В. Сети и системы передачи информации: учебное издание / Костров Б. В., Ручкин В. Н. - Москва: Академия, 2021 - 256 с. (Специальности среднего профессионального образования).

3. Кутузов, О. И. Инфокоммуникационные системы и сети: учебник для спо / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021 — 244 с. — ISBN 978-5-8114-8488-1.
4. Соснин, П. И. Архитектурное моделирование автоматизированных систем / П. И. Соснин. — 3-е изд., стер. — Санкт-Петербург: Лань, 2023 — 180 с. — ISBN 978-5-507-46075-
5. Уймин, А. Г. Практикум. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование / А. Г. Уймин. — Санкт-Петербург: Лань, 2024 — 116 с. — ISBN 978-5-507-48647-2.
6. Хабаров, С. П. Основы моделирования беспроводных сетей. Среда OMNeT++: учебное пособие для спо / С. П. Хабаров. — Санкт-Петербург: Лань, 2021 — 260 с. — ISBN 978-5-8114-6968-0.
7. Хабаров, С. П. Основы моделирования технических систем. Среда Simintech / С. П. Хабаров, М. Л. Шилкина. — 2-е изд., стер. — Санкт-Петербург: Лань, 2024 — 120 с. — ISBN 978-5-507-47414-1.

Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибер безопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ.URL: http://bit.mephi.ru/

Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru–
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11. Федеральный портал «Российское образование www.edu.ru

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, 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	
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	

ПК1.4. 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	
ОК 1 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	
ОК 2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 9 Пользоваться профессиональной документацией на государственном и иностранном языках	эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	

Приложение
к программе СПО10.02.05
Обеспечение информационной безопасности
Автоматизированных систем

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

2024г.

СОДЕРЖАНИЕ

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

Цель и планируемые результаты освоения профессионального модуля

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 профессиональных компетенций
ВД2	**Защита информации в автоматизированных системах программными и программно-аппаратными средствами**
ПК2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК2.6.	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.

Общие компетенции

Код	**Наименование видов деятельности и профессиональных компетенций**
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках

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 отказови 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 гарантированногоуничтожения информации; −устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; −осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
знать	− 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.

Количество часов ,отводимое на освоение профессионального модуля

Всего часов ___**534**_____
в том числе в форме практической подготовки - 332 часа

Из них на освоение МДК - **342** часов
в том числе самостоятельная работа_____14_____
промежуточная аттестация по МДК _____12_____
практики, в том числе учебная - **72** часов
производственная - **108**часов
Промежуточная аттестация – экзамен по модулю – **12** часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час	В т.ч. в форме практической. подготовки	Объем профессионального модуля, ак. час.								
				Обучение по МДК							Практики	
				Всего	В том числе						Учебная	Производственная
					Теоретическое обучение	Лаборат. и практ. занятий	Курсовых работ (проектов)	самостоятельная работа	Консультации	Промежуточная аттестация		
1	2	3	4	5	6		7	8	9	10	11	12
ПК 2.1– ПК 2.6 ОК 1, ОК 2, ОК9	**Раздел 1модуля.** Применение программных и программно-аппаратных средств защиты информации	**186**	76	**186**	68	76	30	12				
	Раздел 2 модуля. Применение криптографических средств защиты информации	**156**	64	**156**	66	64		14	6	6		
	Учебная практика, часов	**72**	72								72	
	Производственная практика, часов	**108**	108									108
	Промежуточная аттестация	**12**	12									
	Всего:	**534**	332	**342**	134	140	30	26	6	6	**72**	**108**

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 1модуля. Применение программных и программно-аппаратных средств защиты информации		**186**
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**186**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**	**2**
	Предмет и задачи программно-аппаратной защиты информации	
	Основные понятия программно-аппаратной защиты информации	
	Классификация методов и средств программно-аппаратной защиты информации	
Тема 1.2. Стандарты безопасности	**Содержание**	**4**
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требованияирекомендациипозащитеинформациипрограммнымиипрограммно-аппаратными средствами. Профилизащитыпрограммныхипрограммно-аппаратныхсредств (межсетевыхэкранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	
	Стандартыпозащитеинформации,всоставкоторыхвходяттребованияирекомендациипо защите информациипрограммнымиипрограммно-аппаратнымисредствами.	
	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	**Содержание**	**4**

автоматизированная система	Автоматизация процесса обработк иинформации	
	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	**6**
	Учет, обработка, хранение и передача информациив АИС	
	Ограничение доступа на входв 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	
Тема1.4. 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	**6**
	Распределение каналов в соответствии с источниками воздействия на информацию	
Тема 1.5. Принципы программно-аппаратной защиты информации от	**Содержание**	**4**
	Понятие несанкционированного доступа к информации	
	Основные подходы к защите информации от НСД	

несанкционированного доступа	Организация доступа к файлам ,контроль доступа и разграничение доступа, и ерархический доступ к файлам.Фиксация доступа к файлам	
	Доступ к данным со стороны процесса	
	Особенности защиты данных от изменения. Шифрование.	
	Тематика практических занятий и лабораторных работ	**6**
	Организация доступа к файлам	
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	
Раздел 2. Защита автономных автоматизированных систем		
Тема 2.1.Основы защиты автономных автоматизированных систем	**Содержание**	**4**
	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**	**4**
	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**	**4**
	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. Другиео бъекты, 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	**4**
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	
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 на примере MSOffice	
	Тематика практических занятий и лабораторных работ	**4**
	Защита информации от несанкционированного копирования с использованием специализированных программных средств	
	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	
Тема 2.5. Защита информации на машинных носителях	**Содержание**	**4**
	Проблема защиты от чуждаемых 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 прирасследовании инцидентов. Нормативная база, документирование результатов	
	Безвозвратное удалениеданных. Принципы и алгоритмы.	
	Тематика практических занятий и лабораторных работ	**8**

	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**	**2**
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	
	Устройства Touch Memory	
Тема 2.7. Системы обнаружения атаки 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.	
	Тематика практических занятий и лабораторных работ	**4**
	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	
Раздел3.Защитаинформациивлокальныхсетях		
Тема 3.1. Основы построения защищенных сетей	**Содержание**	**4**
	Сети, работающие по технологии коммутации пакетов	
	Стек протоколов TCP/IP. Особенности маршрутизации.	
	Штатные средства защиты информации стека протоколов TCP/IP.	
	Средства идентификации аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	
Тема3.2.Средства организации VPN	**Содержание**	**4**
	Виртуальная частная сеть. Функции, назначение, принцип построения	
	Криптографическиеи 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	**4**
	Развертывание VPN	
Раздел4. Защитаинформациивсетяхобщегодоступа		
Тема4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание**	**4**
	Методы защиты информации и 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 телепакетов 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	**6**
	Изучение и сравнение архитектур DualHomedHost, BastionHost, Perimetr.	
	Изучение различных способов закрытия "опасных" портов	
Раздел 5.Защита информации в базах данных		
Тема 5.1. Защита информации в базах данных	**Содержание**	**4**
	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 к риптографических средств защиты информации и в базах данных	
	Тематика практических занятий и лабораторных работ	**6**
	Изучение механизмов защиты СУБДMSAccess	

	Изучение штатных средств защиты СУБДMSSQLServer	
Раздел 6. Мониторинг систем защиты		
Тема 6.1.Мониторинг систем защиты	**Содержание**	**4**
	Понятие и обоснованиене обходимости использования мониторинга как необходимой компоненты системызащиты 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	
	Источникии нформации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	
	Классификация сетевых мониторов	
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
	Тематика практических занятий и лабораторных работ	**4**
	Изучение и сравнительный анализ распространенных сетевых мониторов напримере RealSecure, SNORT, NFR или других аналогов	
	Проведение аудита ЛВС сетевым сканером	
Тема6.2.Изучение мер защиты информации в информационных системах	**Содержание**	**2**
	Изучение требований о защите информации, несоставляющей государственную тайну. Изучение методических документо в ФСТЭК по применению мер защиты.	
	Тематика практических занятий и лабораторных работ	**4**
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	
Тема6.3.Изучение современных программно-аппаратных комплексов.	**Тематика практических занятий и лабораторных работ**	**8**
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol8 или других	

	аналогов	
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов	
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов	
	Изучение функционала и областей применения DLP систем на примереI nfoWatchTrafficMonitor или Других аналогов	
Курсовая работа		**30**
1 Методические рекомендации по написанию курсовой работы. Выбор темы. 2 Работа над введением: актуальность выбранной темы, цели и задачи курсовой работы 3 Работа над 1 разделом курсовой: подбор литературы, Интернет-ресурсов. 4 Работа над 1 разделом курсовой: изучение теоретической основы темы, оформление 5 Работа над 2 разделом курсовой: изучение особенностей темы, изучение необходимых для проекта документов 6 Работа над заключительной частью курсовой работы 7 Оформление текстовой части. 8 Работа над речью для защиты курсовой работы. 9 Работа над презентацией для защиты курсовой работы 10 Защита курсовой работы.		2 4 4 4 4 4 2 2 2 2
Примерная 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. Обзорсовременныхпрограммныхипрограммно-аппаратныхсредств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты		**12**
Промежуточная аттестация по МДК.02.01 дифференцированный зачет		**2**

Раздел 2 модуля Применение криптографических средств защиты информации		**156**
МДК.02.02. Криптографические средства защиты информации		**156**
Введение	**Содержание**	**2**
	Предмет и задачи криптографии. История криптографии. Основные термины	
Раздел 1. Математические основы защиты информации		
Тема 1.1. Математические основы криптографии	**Содержание**	**12**
	Элементы теории множеств. Группы, кольца, поля.	
	Делимость чисел. Признаки делимости. Простые и составные числа.	
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	
	Классы. Полная и приведенная система вычетов.Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм	
	быстрого возведения в степень по модулю.	
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	
	Китайская теорема об остатках.	
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	Арифметические операции над большими числами.	
	Эллиптические кривые и их приложения в криптографии.	
	Тематика практических занятий и лабораторных работ	**6**
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	
	Проверка чисел на простоту	
	Решение задач с элементами теории чисел.	
Раздел 2. Классическая криптография		
Тема 2.1. Методы криптографической защиты информации	**Содержание**	**8**
	Классификация основных методов криптографической защиты. Методы симметричного шифрования	
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	
	Методы перестановки. Табличная перестановка, маршрутная перестановка	

	Гаммирование. Гаммирование с конечной и бесконечной гаммами	
	Тематика практических занятий и лабораторных работ	**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, квантовый криптоанализ.	
	Тематика практических занятий и лабораторных работ	**10**
	Криптоанализ шифра простой замены методом анализа частотности символов	
	Криптоанализ классических шифров методом полного перебора ключей	
	Криптоанализ шифра Вижинера	
Тема 2.3. Поточные шифры и генераторы псевдослучайныхчисел	**Содержани еучебного материала**	**4**
	Основные принципы поточногошифрования. Применение генераторов ПСЧ в криптографии	
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	Тематика практических занятий и лабораторных работ	**2**
	Применение методов генерации ПСЧ	
Раздел3. Современнаякриптография		
Тема3.1.Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	**6**
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	
	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	
	Тематика практических занятий и лабораторных работ	**8**
	Кодирование информации	
	Программная реализация классических шифров	
	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	
Тема3.2.Симметричные системы шифрования	**Содержание учебного материала**	**4**
	Общие сведения. Структурная схема симметричных криптографических систем	

	Отечественные алгоритмы Магма и Кузнечики стандарты ГОСТР34.12-2015 и ГОСТР34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	
	Тематика практических занятий и лабораторных работ	**4**
	Изучение программной реализации современных симметричных шифров	
Тема3.3.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**
	Применение различных асимметричных алгоритмов.	
	Изучение программной реализации асимметричного алгоритма RSA	
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебногоматериала**	**4**
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Тематика практических занятий и лабораторных работ	**8**
	Применение различных функций хеширования, анализ особенностей хешей	
	Применение криптографических атак на хеш-функции.	
	Изучение программно-аппаратных средств, реализующих основные функции ЭП	
Тема3.5.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.	
Тема3.6.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 802.11с 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	
Тема3.8.Компьютерная стеганография	**Содержани еучебного 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	**6**
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	
	Реализация простейших стеганографических алгоритмов	
Примерная тематика самостоятельной работы при изучении МДК.02.02 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии		**14**
Консультации		**6**
Промежуточная аттестация по МДК.02.02 экзамен		**6**

Учебная практика **Виды работ:** −Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах − Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности − Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности − Составление документации по учету, обработке, хранению и передаче конфиденциальной информации − Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации − Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. − Устранение замечаний по результатам проверки −Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. −Применение математических методов для оценки качества и выбора наилучшего программного средства − Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	**72**
Производственная практика **Виды работ** – Анализ принципов построения систем информационной защиты производственных подразделений. – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении – Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	**108**
Консультации **Экзамен по модулю**	**6** **6**
Всего:	**534**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

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

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

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

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

Информационноеобеспечениеобучения

3.2.1Основныепечатныеисточники:

1. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва: Академия, 2021 -336 с. (Специальности среднего профессионального образования).
2. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум: учебное пособие для спо / Р. Н. Гилязова. — 3-е изд., стер. — Санкт-Петербург: Лань, 2022 — 44 с. — ISBN 978-5-8114-9138-4.
3. Глухов, М. М. Введение в теоретико-числовые методы криптографии / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 3-е изд., стер. — Санкт-Петербург: Лань, 2024 — 396 с. — ISBN 978-5-507-47388-5.
4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования/ О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2023 — 312 с. —(Профессиональное образование). — ISBN 978-5-534-13221-2.
5. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021 — 96 с. — ISBN 978-5-8114-7906-1.
6. Никифоров, С. Н. Методы защиты информации. Защищенные сети: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021 — 96 с. — ISBN 978-5-8114-7907-8.
7. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021 —124 с. — ISBN 978-5-8114-8256-6.

8. Никифоров, С. Н. Методы защиты информации. Шифрование данных: учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022 — 160 с.— ISBN 978-5-507-44449-6.
9. Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для спо /. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022 — 108 с. — ISBN 978-5-8114-9038-7.
10. Прохорова, О. В. Информационная безопасность и защита информации: учебник для спо / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург: Лань, 2023 — 124 с. — ISB 978-5-507-47174-4.
11. Щербак, А. В. Информационная безопасность: учебник профессионального образования / А. В. Щербак. — Москва: Издательство Юрайт, 2024 — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3.

Периодические издания:

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

Электронные источники:

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

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемыев 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, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК2.2.Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системахотдельными 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, хранениии 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) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	
ОК 1 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	
ОК 2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 9 Пользоваться профессиональной документацией на государственном и иностранном языках	эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	

Приложение
к программе СПО10.02.05
Обеспечение информационной безопасности
Автоматизированных систем

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

2024г.

СОДЕРЖАНИЕ

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

Цель и планируемые результаты освоения профессионального модуля

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

Код	Наименованиевидовдеятельностиипрофессиональныхкомпетенций
ВД3	**Защитаинформациитехническимисредствами**
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.

Общие компетенции:

Код	Наименованиевидовдеятельностиипрофессиональныхкомпетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках

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 информациии носителей информации; − применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; − применять технические средства для защиты информации вусловиях 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; −основныес пособы физической защиты объектов информатизации; −номенклатуру применяемых средств физической защиты объектов информатизации.

Количество часов, отводимое на освоение профессионального модуля

Всего часов ___**522**_____

в том числе в форме практической подготовки - 350 часов

Из них на освоение МДК - **330** часов

в том числе самостоятельная работа_____24_____

промежуточная аттестация по МДК _____12_____

практики, в том числе учебная - **72** часов

производственная - **108**часов

Промежуточная аттестация – экзамен по модулю – **12** часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Структура профессионального модуля ПМ.03 Защита информации техническими средствами

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час	В т.ч. в форме практической. подготовки	Объем профессионального модуля, ак. час.								
				Обучение по МДК							Практики	
				Всего	В том числе						Учебная	Производственная
					Теоретическое обучение	Лаборат. и практ. занятий	Курсовых работ (проектов)	самостоятельная работа	Консультации	Промежуточная аттестация		
1	2	3	4	5	6		7	8	9	10	11	12
ПК3.1-ПК.3.5 ОК 1, ОК 2, ОК9	**Раздел 1модуля.** Применение технической защиты информации	**170**	80	**170**	68	80		10	6	6		
	Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации	**160**	78	**160**	38	78	30	14	6	6		
	Учебная практика, часов	**72**	72								72	
	Производственная практика, часов	**108**	108									108
	Промежуточная аттестация	**12**	12									
	Всего:	**522**	350	**522**	106	158	30	24	12	12	**72**	**108**

Тематический план и содержание профессионального модуля

Наименование разделовитем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение технической защиты информации		**170**
МДК.03.01 Техническая защита информации		**170**
Раздел 1. Концепция инженерно-технической защиты информации		
Тема1.1. 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**	**6**
	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		
Тема 2.1.Информация как предмет защиты	**Содержание**	**6**
	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 противодействию технической разведке.	
	Тематика практических занятий и лабораторных работ	**6**

	Содержательный анализ основных руководящих, нормативных и методических документов по защите информациии противодействию технической разведке.	
Тема2.2.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 практически хзанятий и лабораторных работ	**6**
	Классификация демаскирующих признаков. Основные виды угроз информации. Обоснование выбора кабинета как объекта защиты. Составление плана кабинета как объекта защиты.	
Тема 2.3. Методы и средства технической разведки	**Содержание**	**4**
	Классификация технических средств разведки. Методы и средства технической разведки. Средства не санкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Тематика практически хзанятий и лабораторных работ	**4**
	Типовая структура технических каналов утечки. Моделирование каналов утечки утечки информации. Методы добавления информации о вещественных носителях. Дистанционный анализ веществ.	
Раздел3.Физическиеосновытехническойзащитыинформации		
Тема3.1.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 их характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика практически хзанятий и лабораторных работ	**4**
	Измерение параметров физических полей Защита от утечки по акустическому каналу.	
Тема 3.2. Физические процессы при Подавлении опасных сигналов	**Содержание**	**2**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Тематика практически хзанятий и лабораторных работ	**4**

	Энергетическое скрытие акустических сигналов:звукоизоляция и звукопоглащение.	
Раздел4.Системы защиты от утечки информации		
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 практически хзанятий 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. Номенклатур апримeняемых средств защиты информации от несанкционированной утечки по проводномуканалу.	
	Тематика практически хзанятий и лабораторных работ	**4**
	Защита от утечки по проводному каналу	
Тема4.3.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 практически хзанятий и лабораторных работ	**4**
	Защита от утечки по виброакустическому каналу	
Тема4.4.Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**4**
	Прослушивание информации от радио телефонов. 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 практически хзанятий и лабораторных работ	**8**

	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	
Тема4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**4**
	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 практически хзанятий и лабораторных работ	**4**
	Защита от утечки по телефонному каналу	
Тема4.6.Системы защиты от утечки информации по электросетевомуканалу	**Содержание**	**4**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от есанкционированной утечки по электросетевому каналу..	
	Тематика практически хзанятий и лабораторных работ	**4**
	Защита от утечки по электросетевому каналу	
Тема 4.7. Системы защиты от утечки информации по оптическомуканалу	**Содержание**	**2**
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Тематика практически хзанятий и лабораторных работ	**2**
	Защита от утечки по оптическому каналу	
Раздел5. Применение и эксплуатация технических средств защиты информации		
Тема5.1.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.	
	Тематика практически хзанятий и лабораторных работ	**10**

	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.	
Тема5.2.Эксплуатация технических средств защиты информации	**Содержание**	**8**
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.	
	Тематика практически хзанятий и лабораторных работ	**12**
	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.	
Примерная тематика самостоятельной учебной работы 1 Направление комплексного проектирования систем защиты информации 2 Основные проблемы реализации систем защиты информации 3 Требования к КСЗИ 4 Задачи стратегии защиты информации 5 Верификация 6 Дискреционный контроль доступа 7 Биометрическая идентификация 8 Биометрия по клавиатурному почерку 9 Классификация признаков голоса и речи 10 Средства высоконадежной биометрической аутентификации 11 Шпионаж, сбор служебной информации, сканирование эфира, обработка неучтенных источников		**10**
Консультации **Промежуточная аттестация по МДК.03.01 экзамен**		**6** **6**
Раздел 2модуля. Применение инженерно-технических средств физической защиты объектов информатизации		**160**
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**160**
Раздел1.Построение и основные характеристики инженерно-технических средств физической защиты		
Тема1.1.Цели и задачи физической защиты объектов информатизации	**Содержание**	**4**
	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 практически хзанятий и лабораторных работ Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.	**2**
	Тематикаучебныхзанятийформируетсяобразовательнойорганизацией самостоятельно	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**4**
	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 практически хзанятий и лабораторных работ	**10**
	Рассмотрение инженерных конструкций, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**4**
	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 практически хзанятий и лабораторных работ	**12**
	Монтаж датчиков пожарной и охранной сигнализации	
Тема 2.2. Система контроля и управления доступом	**Содержание**	**6**
	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 практически хзанятий и лабораторных работ	**8**
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема2.3.Система	**Содержание**	**4**

телевизионного наблюдения	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения.Составсистемытелевизионногонаблюдения.Видеокамеры.Объективы.Термокожухи. Поворотныесистемы.Инфракрасныеосветители.Детекторыдвижения.	
	Тематика практически хзанятий и лабораторных работ	**8**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Тема2.4.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 практически хзанятий и лабораторных работ	**6**
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема2.5Система воздействия	**Содержание**	**2**
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	
	Тематика практически хзанятий и лабораторных работ	**8**
	Определение основных показателей технических средств воздействия	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 3.1Применение инженерно-технических средств физической защиты	**Содержание**	**6**
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийнымоборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП.	
	Тематика практически хзанятий и лабораторных работ	**12**
	Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия	
Тема3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**2**
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.	
	Тематика практически хзанятий и лабораторных работ	**12**
	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.	
Курсовой проект (работа)	**30**
1 Методические рекомендации по написанию курсовой работы. Выбор темы. 2 Работа над введением: актуальность выбранной темы, цели и задачи курсовой работы 3 Работа над 1 разделом курсовой: подбор литературы, Интернет-ресурсов. 4 Работа над 1 разделом курсовой: изучение теоретической основы темы, оформление 5 Работа над 2 разделом курсовой: изучение особенностей темы, изучение необходимых для проекта документов 6 Работа над заключительной частью курсовой работы 7 Оформление текстовой части. 8 Работа над речью для защиты курсовой работы. 9 Работа над презентацией для защиты курсовой работы 10 Защита курсовой работы.	2 4 4 4 4 4 2 2 2 2
Примерная тематика самостоятельной работы 1 Понятие об информации и объектах информатизации. Физические свойства и характеристики информационных сигналов. 2 Нормативно-правовая база защиты объектов информатизации. Роль и место правового обеспечения физической защиты объектов информатизации. 3 Жизненный цикл системы инженерно-технических средств физической защиты. Основные методы внедрения инженернотехнических средств по объектам информатизации. 4 Основные этапы и маршруты проникновения к объектам информатизации. Групповые и одиночные маршруты проникновения на объекты. 5 Требования к инженерно-техническим средствам физической защиты объектов информатизации по обеспечению информационной безопасности предприятия. 6 Основные понятия и определения. Классификация комплексов инженерно-технических средств. Основные параметры по информационной безопасности на объектах. 7 Принцип построения интегрированных систем охраны информации на объектах. 8 Общая характеристика методов хищения информации, копирования, уничтожения, искажения, подавления информации. Утечка информации по каналам ПЭМРШ. 9 Классификация методов технической разведки. Способы ведения разведки на объектах информатизации. 10.Телевизионные датчики и телеохранные системы. Промышленные телевизионные установки контроля и охраны объекта информатизации. 11.Технические характеристики видеокамер охранного назначения. Наименования, классификация, форм-фактор камер охранного назначения.	**14**
Промежуточная аттестация поМДК.03.02 дифференцированный зачет	**2**

Учебная практика **Виды работ:** - Измерение параметров физических полей. - Определение каналов утечки ПЭМИН. - Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. - Установка и настройка технических средств защиты информации. - Проведение измерений параметров побочных электромагнитных излучений и наводок. - Проведение аттестации объектов информатизации. - Монтаж различных типов датчиков. - Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. - Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. - Рассмотрение системы контроля и управления доступом. - Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. - Рассмотрение датчиков периметра, их принципов работы. - Выполнение звукоизоляции помещений системы зашумления. - Реализация защиты от утечки по цепямь электропитания и заземления. - Разработка организационных и технических мероприятий по заданию преподавателя; - Разработка основной документации по инженерно-технической защите информации.	***72***
Производственная практика **Виды работ** 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	***108***
Консультации ***Экзамен по пмодулю***	**6** **6**
Всего	***522***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГ ОМОДУЛЯ

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

Лекционные аудитории с мультимедийным оборудованием; лаборатория «Техническихсредствзащитыинформации».

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

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

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

Информационное обеспечение обучения

Основные печатные издания

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2019.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2020
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2018. – 172 с.
4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2018 – 336с

Основные электронные издания

1. Введение в теоретико-числовые методы криптографии : учебное пособие для спо / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 396 с. — ISBN 978-5-507-45348-1. —
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, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8.
3. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие для спо / Р. Н. Гилязова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 44 с. — ISBN 978-5-8114-9138-4.
4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального

образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.

5. Полякова, Т. А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2.

6. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-47174-4.

7. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3.

Дополнительные источники

1. Котеров Д.В. PHP 5 в подлиннике. – СПб.: БХВ-Петербург, 2018. – 1104 с.

2. Федеральный образовательный портал «Информационно –коммуникационные технологии в образовании».

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, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	
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	
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 3.4 Осуществлять измерениепараметров фоновых шумов, а также физических полей,создаваемых техническими средствамизащиты информации	Проводитьсамостоятельныеизмерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	

ПК3.5Организовывать отдельные работы по физической защите объектов информатизации	Проявлятьзнанияввыборе способоврешениязадачпо организации отдельных работпофизической защите объектов информатизации	
ОК 1.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	
ОК 2.Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 9.Пользоваться профессиональной документацией на государственном и иностранном языках	эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	

Приложение
к программе СПО10.02.05
Обеспечение информационной безопасности
Автоматизированных систем

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

2024г.

СОДЕРЖАНИЕ

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

Цель и планируемые результаты освоения профессионального модуля

В результате изучения программы профессионального модуля студент должен освоить выполнение работ по профессии 16199 «Оператор электронно-вычислительных и вычислительных машин» и соответствующие ему общие и профессиональные компетенции.

Код	Наименованиевидовдеятельностиипрофессиональныхкомпетенций
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

Общие компетенции:

Код	Наименованиевидовдеятельностиипрофессиональныхкомпетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках

В результате освоения профессионального модуля студент должен:

Иметь практический	выполнения требований техники безопасности при работе с вычислительной техникой; организации рабочего места оператора электронно-вычислительных и вычислительных машин подготовки оборудования компьютерной системы к работе; инсталляции, настройки и обслуживания программного обеспечения компьютерной управления файлами; применения офисного программного обеспечения в соответствии с прикладной задачей; решения проблем технического и программного обеспечения связанных с организацией ввода/вывода цифровой информации

опыт	вычислительнойтехникой; –организациирабочегоместаоператораэлектронно-вычислительных и вычислительных машин; –подготовкиоборудованиякомпьютернойсистемы к работе; –инсталяции,настройкиииобслуживанияпрограммногообеспечения компьютерной системы; –управления файлами; –применения офисного программного обеспечения в соответствии с прикладной задачей; –использованияресурсовлокальнойвычислительнойсети; –использованияресурсов,технологийи сервисов Интернет; –применениясредств защитыинформациивкомпьютернойсистеме.
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; – создаватьиуправлятьсодержимымпрезентацийспомощью редакторов презентаций; – использовать мультимедиа проектор для демонстрации презентаций; – вводить, редактировать и удалять записи в базе данных; – эффективно пользоваться запросами базы данных; –создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; – производить сканирование документов и их распознавание; – производить распечатку, копирование и тиражирование документов на принтере и других устройствах; – управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; – осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; – осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; – осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; –осуществлять резервное копирование и восстановление данных.

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; −основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.

Количество часов, отводимое на освоение профессионального модуля

Всего часов ___**408**_____

в том числе в форме практической подготовки - 408 часов

Из них на освоение МДК - **108** часов

в том числе самостоятельная работа_____6_____

промежуточная аттестация по МДК _____12_____

практики, в том числе учебная - **180** часов

производственная - **108**часов

Промежуточная аттестация – экзамен по модулю – **12** часов

2. СТРУКТУРАИСОДЕЖАНИЕУЧЕБНОЙ ДИСЦИПЛИНЫ

Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час	В т.ч. в форме практической. подготовки	Объем профессионального модуля, ак. час.							
				Обучение по МДК						Практики	
				Всего	В том числе					Учебная	Производственная
					Теоретическое обучение	Лаборат. и практ. занятий	самостоятельная работа	Консультации	Промежуточная аттестация (экзамен по МДК)		
1	2	3	4	5	6	7	8	9	10	11	12
ПК4.1–ПК 4.4. ОК 1, ОК 2, ОК 9	**Раздел1модуля**.Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»	**108**	108	**108**	14	76	6	6	6		
	Учебная практика	**180**	180							180	
	Производственная практика, часов	**108**	108								108
	Промежуточная аттестация (экзамен по модулю)	**12**	12								
	Всего:	**408**	408	**108**	104	76	6	6	6	**180**	**108**

Тематическийпланисодержаниеучебной дисциплины

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержаниеучебного 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»		**108**
Тема 1.1. Техника безопасности при работе с ПК	**Содержание**	**2**
	Нормативные документы по охране труда приработе с ПК, переферийным, мультимедийным оборудованием и компьютерной оргтехникой. Организация рабочего места и санитарные нормы при работе с ПК	
Тема 1.2. Основные принцыпы работы ПК и периферийных устройств	**Содержание**	**2**
	Архитектура и принципы работы основных логических блоков персонального компьютера, организация и принцип работы памяти, взаимосвязь с периферийными устройствами, организация и режимы работы процессора, использование прерываний. Взаимодействие внутренних устройств ПК. Правила эксплуатации расходных материалов и сменных компонентов. Носители информации: виды и основные принципы работы	
	Тематика практических занятий и лабораторных работ	12
	Настройка параметров функционирования ПК Подключение периферийных устройств. Классификация портов и разъемов, установка драйверов. Способы подсоединения периферийных устройств. Подсоединение периферийных устройств по сети. Установка и замена расходных материалов для периферийных устройств: виды расходных материалов, методы установки. Сроки эксплуатации.	
Тема 1.3. Системное и прикладное ПО	**Содержание**	**2**
	ПО, его виды, функции, типы, классификация	
	Тематика практических занятий и лабораторных работ	8
	Установка операционной системы Настройка интерфейса ОС (рабочий стол, безопасность стстемы, подключение к сети) Установка прикладных программ: пакет Microsoft Office, архиватор, веб-браузер	

Тема 1.4. Диагностика неисправной системы	**Содержание**	**2**
	Оформление отчетгной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации компьютера	
	Тематика практических занятий и лабораторных работ	8
	Диагностика простейших неисправностей ПК Устранение простейших неисправностей ПК Устранение простейших неисправностей периферийного оборудования Устранение простейших неисправностей организационной техники	
Тема 1.5. Выполнение ввода и обработки текстовой информации. Технология обработки числовой информации	**Содержание**	**2**
	Технологии обработки текстовой информации. Технология обработки числовой информации. Форматы данных. Способы ввода и оформления данных. Использование различных способов ввода и оформления данных по заданным условиям	
	Тематика практических занятий и лабораторных работ	16
	Таблицы в текстовых редакторах Формирование больших документов Форматирование стмволов и абзацев Создание и форматирование таблиц по заданным условиям Использование расчетных операций в таблицах. Построение диаграмм. Вставка гиперссылок, сносок, указателей, закладок Распечатка, копирование и тиражирование готового документа на принтере и других кстройствах Графические объекты в электронных таблицах. Организация расчетов в электронных таблицах. Обработка таблиц как баз данных. Построение диаграмм по заданным условиям. Расширенная фильтрация и условное форматирование. Использование возможностей ЭТ по поиску решения.	
Тема 1.6 Технологии создания мультимедийных презентаций. Технологии обротки графической информации	**Содержание**	
	Тематика практических занятий и лабораторных работ	8
	Основы работы со слайдом в MS PowerPoint. Анимация объектов. Создание автоматической презентации Создание презентации с применением триггеров. Создание и редактирование изображений Вопроизведение презентации с использованием мультмедиа проектора.	

Тема 1.7 Базы данных Компьютерные сети	**Содержание**	**2**
	Проектирование БД. Модели организации БД. Основы работы в СУБД MS Access. Классификация и назначение компьютерных сетей. Каналы связи и средства коммутации. Програмое обеспечение для работы в компьютерных сетях. Сетевое программное обеспечение	
	Тематика практических занятий и лабораторных работ	6
	Ввод, редактирование и удаление записи в базе данных. Создание базы данных, состоящей из нескольких таблиц.Создание и использование запросов базы данных. Создание форм и отчетов	
Тема 1.8 Глобальная компьютерная сеть Интернет	**Содержание**	
	Тематика практических занятий и лабораторных работ	10
	Программное обеспечение для работы с ресурсами Интернета: инсталляция, принцип работы, деинсталляция. Навигация по Веб-ресурсам Интернета с помощью браузера. Поиск информации с помощью интернет сайтов. Определение IP-адреса Поиск документа в базе данных поисковой системы с помощью введения запроса. Сортировка и анализ информации поисковых интернет сайтов. Справочно-поисковые сети Интернет Интернет-технологии как техническая основа интеграции образоывательных ресурсов, доступа к образоывательным ресурсам и применения дистанционных форм в образовательной деятельности. Создание и обмен письмами электронной почты. Поиск,сортировка и анализ информации с помощью поисковых интернет сайтов. Пересылка и публикация файлов данных в Интернете.	
Тема 1.9 Защита информации при работе с офисными приложениями	**Содержание**	**2**
	Категории компьютерных вирусов. Основные средства защиты от вредоносного ПО и несанкционированного доступа к защищаемым ресурсам ПК.	
	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. Работа с интивирусными программами Разграничение прав доступа в сети Резервное архивирование и восстановление опреационной системы	

Самостоятельная работа по разделу Создание обобщающей презенции по теме «Основы работы с пакетами прикладных программ»	**6**
Промежуточная аттестация Консультации Экзамен по МДК	 **6** **6**
УП.04. Учебная практика **Виды работ:** 1. Соблюдение техники безопасности при работе на ЭВМ 2. Изучение архитектуры ЭВМ, структуры и основных принципов ЭВМ 3. Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка 4. Устанвка и замена расходных материалов для принтеров, ксерокса, плоттера. 5. Выбор рациональной конфигурации оборудования в соответствии с решаемой задачей 6. Установка операционной среды, настройка интерфейса ОС (рабочий стол, безопасность системы, подключение к сети) 7. Установка прикладных программ 8. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете 9. Диагностика простейших неисправностей ПК, периферийного оборудования и компьютерной оргтехники 10. Офрмление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ 11. Сканирование текстовых документов и их распознование 12. Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов 13. Форматирование и редактирование документов в текстовом процессоре 14. Работа с таблицами в текстовом процессоре 15. Работа с диаграммами в текстовом процессоре 16. Работа с графическими объектами в текстовом процессоре 17. Печать документов в текстовом процессоре 18. Создание и форматирование таблицы в редакторе электронных таблиц 19. Вычисление с помощью формул в электронной табльце 20. Работа со встроенными функциями в электронных таблиц 21. Работа со списками в электронной таблице 22. Создание форм для ввода данных в таблицы 23. Создание и работа с диаграммами и графиками 24. Обмен данными между текстовым процессором и электронной таблицей 25. Работа с расширенной фильтрацией и условным форматированием 26. Построение презентации различными способами 27. Обработка объектов слайдов презентации 28. Настройка анимации объектов	**180**

29. Настройка показа и демонстрация результатов работы средствами мультимедиа 30. Применение триггеров при создании презентации 31. Ввод данных в таблицы базы данных 32. Создание простых запросов без параметров и с параметрами. Создание отчетов. 33. Создание форм и их защита 34. Создание связей таблиц по типу многи-ко-многим 35. Рисование объектов средствами графического редактора 36. Работа с залифками и контурами впрограмме векторной графики 37. Работа с текстом в программе векторной графики 38. Работа с эффектами в програмее векторной графики 39. Вставка и редактирование готового изображения с использованием программ растровой графики 40. Работа с цветом с использованием программ растровой графики 41. Работа со слоями с использованием программ растровой графики 42. Работа со спецэффектами с использованием программ растровой графики 43. Создание программы в графическом редакторе 44. Создание и обмен письмами электронной почты 45. Новигация по Веб-ресурсам интернета с помощью программы Веб-браузера 46. Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов 47. Пересылка и публикация файлов данных в интернете 48. Использование штатных средств защиты операционной системы и прикладных программ 49. Применение парольной защиты 50. Установка антивирусных программ. Их настройка. Обновление базы. 51. Выполнение архивирования данных 52. Выполнение резервного копирования и восстановления данных 53. Организация работ по использованию и применению политики безопасности организации 54. Персонализация работы антивирусных программ 55. Организация мероприятий по резервному восстановлению данных 56. Использование сервисов сети Интернет в профессиональной деятельности 57. Применение программ средств для мониторинга трафика.	
Производственная практика **Виды работ** 1. Техника безопасности при работе с вычислительной техникой: изучение нормативной документации. Организация рабочего места оператора электронно-вычеслительных и вычеслительных машин: учет антропометрических данных, выбор рациональной рабочей поверхности, физиологически рациональной рабочей позы, оргтехоснастка, защита от блескости 2. Подклюмение блоков персонального компьютера и приферийных устройств: конструктивы (разъемы), основные характеристики 3. Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка	**108**

4. Установка операционной системы, настройка интерфейса ОС: специальные возможности и дополнительные параметры 5. Инсталляция дополнительного программного обеспечения: особенности специализированного прикладного программного обеспечения 6. Настройка системного и прикладного программного обеспечения в соответствии с прикладной задачей 7. Установка и замена расходных материалов для принтеров, ксерокса, плоттера 8. Диагностика простейших неисправностей ПК: блок питания, материнская плата, оперативная память, видеокарта, центральный процессор, конденсаторы 9. Диагностика простейших неисправностей периферийного оборудования и компьютерной оргтехники: выявление устройств, вышешдгших из сторя, и подбор для них подходящей замены 10. Создание текстовых документов : создание документов с помощью шаблонов и форм 11. Сканирование документов и их распознование: сканирование прозрачных и непрозрачных оригиналов 12. Распечатка, копирование и тиражирование документов на принтере и других устройствах: произведение копирования документов на различные съемные носители: установка современных приложений беспроводной передачи данных для их последующей печати 13. Создание и редактирование документов организации с применением ЭТ: экспресс-анализ, использование средств для фильтрации данных 14. Обмен данными между текстовым процессором и электронной таблицей в документе: внедрение данных листа в веб-страницу, обмен листами Excel в онлайн-встрече 15. Использование возможностей ЭТ по поиску решения: создание подходящей сводной таблицы, использование нескольких таблиц при анализе данных 16. Создание презентации с применением триггеров: конструктор в PjwerPoint 17. Создание деловой анимированной презентации: создание переходов кинематографического уровня с транформацией 18. Создание бизнес презентации с эффектами анимации. Демонстрация презентации 19. Базы данных организации: создание, заполнение, форматирование. Составление сложных запросов баз данных, Фильтрация данных 20. Создание форм и отчетов с помощью мастера форм базы данных 21. Принцип работы локальной вычислительной сети организации. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети 22. Диагностика и устранение простейших неисправностей при работе в компьютерной сети 23. Новигация по Веб-ресурсам Интернета с помощью браузера: загрузка документа, чтение страницы, переход по гиперссылки, просмотр html-кода 24. Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов 25. Настройка параметров ящика электронной почты организации. Создание и обмен письмами электронной почты 26. Антивирусная защита персонального компьютера с помощью антивирусных программ: настройка брандмауэра, проверка	

файлов в ручном режиме 27. Организация работ по использованию и применеию политики безопасности организации 28. Персонализация работы антивирусных программ 29. Осуществление резервного копирования и восстановления данных: применение облачных сервисов и Drive Backup 30. Организация мероприятий по резервному восстановлению данных 31. Использование сервисов сети Интернет в деятельности организации, применение программных средств для мониторинга трафика	
Консультации **Экзамен квалификационный**	**6** **6**
Всего	**408**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы модуля предполагает наличие лаборатории информационных технологий.

Оборудование лаборатории информационных технологий:

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

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

Учебно-наглядныепособия: схемы, таблицы, учебные презентации

Раздаточный дидактический материал.

Информационноеобеспечениереализациипрограммы

Основныепечатныеисточники:

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

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

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

4. 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, 2021. — 221 с.— ISBN 978-5-4497-0904-2. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL:https://profspo.ru/books/102024

5. Ковган, Н. М. Компьютерные сети: учебное пособие / Н. М. Ковган. — Минск Республиканский институт профессионального образования (РИПО), 2019.— 179 с. — ISBN 978-985-503-947-2. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/93384

6 Колдаев В.Д., Павлова Е.Ю. Сборник задач и упражнений по информатике: учеб. пособие / В.Д. Колдаев, Е.Ю. Павлова; под ред.Л.Г. Гагариной –М.: ИД «ФОРУМ»: ИНФРА-М, 2022

7. Михеева, Е. В. Информационные технологии в профессиональной деятельности: учебник СПО / Е.В. Михеева. - М.: Академия, 2020

8. Михеева, Е. В. Практикум по информационным технологиям в профессиональной деятельности: практ. пособие для СПО / Е. В. Михеева. -М.: Академия, 2020.

9. Новицкий А.П., Организация цифровых вычислительных машин и систем : учебное пособие.-С.Пб: Санкт-Петербургский политехнический университет Петра Великого, 2019.- URL: http://www.iprbookshop.ru/99824.ht ml

10. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д.М. Романенко. — Москва, Вологда : Инфра-Инженерия, 2022. — 460 с. —ISBN 978-5-9729-0962-9. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL:https://profspo.ru/books/124197

Дополнительные источники:

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

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

13.Установка и обслуживание программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования. (СПО) Богомазова Г. Н., 2022, 256с.

14.Аппаратное обеспечение ЭВМ. Практикум. (для ССУЗов) Струмпэ Н.В., Сидоров В.Д. 2022, 160с.
15.Оператор ЭВМ. Практические работы: учеб. пособие для НПО/Н.В. Струмпэ. – 5-е изд., стер. – М.: Издательский центр «Академия», 2024 – 112с.

Электронные источники:

1. Единое окно доступа к образовательным ресурсам: http://window.edu.ru.
2. Центр информационных технологий: http://www.citforum.ru
3. Федеральный центр информационно-образовательных ресурсов:http://fcior.edu.ru
4. Все для программиста: http://www.codenet.ru
5. Информационно-справочный портал: http://www.morepc.ru
6. Беляев А.В. Методы и средства защиты информации: http://www.citforum.ru/internet/infsecure/its2000_01.shtml
7. Лаборатория Касперского – Антивирус: http://www.kaspersky.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	Демонстрировать умения и 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
ПК4.2 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных,работать в графических редакторах	Проявление умения и практическогоопытав работе с текстовыми документами,таблицамии презентациями ,а также базами данных	
ПК4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	Умениепользоваться ресурсамилокальных вычислительных сетей, осуществлятьпоиск,анализ и интерпретацию информации	
ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе	Применение средств защиты информации в компьютернойсистеме	
ОК 1.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	

ОК 2.Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 9.Пользоваться профессиональной документацией на государственном и иностранном языках	эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	