ПРИЛОЖЕНИЕ 1
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНЫХ МОДУЛЕЙ

ОГЛАВЛЕНИЕ

Приложение 1.1
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа профессионального модуля

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

2024 г.

СОДЕРЖАНИЕ

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

1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «эксплуатация автоматизированных (информационных) систем в защищенном исполнении».

Профессиональный модуль включен в обязательную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Планируемые результаты освоения профессионального модуля

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

В результате освоения профессионального модуля обучающийся должен:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК.05	– грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке – проявлять толерантность в рабочем коллективе	– правила оформления документов – правила построения устных сообщений – особенности социального и культурного контекста	
ПК 1.1.	– Выполнять конфигурирование – Настраивать автоматизированные системы в защищенном исполнении – Производить компонент систем защиты информации автоматизированных систем	– 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	– Устанавливать компоненты системы защиты информации автоматизированных (информационных) систем – Настраивать компоненты системы защиты информации автоматизированных (информационных) систем
ПК 1.2.	– Организовывать, конфигурировать, производить монтаж диагностику и устранять неисправности КС – Работать с сетевыми протоколами разных уровней – Осуществлять конфигурирование – Выполнять настройку компонент систем защиты информации автоматизированных систем – Производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации АС	– Теоретические основы компьютерных сетей и их аппаратных – Сетевых моделей – Протоколов и принципов адресации	– Администрировать автоматизированные система в защищенном исполнении

ПК 1.3.	– Настраивать неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным Правилам – Устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным Правилам	– Порядок установки средств защиты информации в компьютерных сетях – Ввод в эксплуатацию средств защиты информации в компьютерных сетях	– Выполнять эксплуатацию компонентов систем защиты информации автоматизированных систем
ПК 1.4.	– Обеспечивать работоспособность – Обнаруживать неисправности – Устранять неисправности	– Принципы основных методов организации – Проведения технического обслуживания вычислительной техники и других технических средств информатизации	– Выполнять диагностику компонентов систем защиты информации автоматизированных систем – Устранять отказы работоспособности автоматизированных (информационных) систем в защищенном исполнении – Восстанавливать работоспособности автоматизированных (информационных) систем в защищенном исполнении

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Трудоемкость освоения модуля

Наименование составных частей модуля	**Объем в часах**	**В т.ч. в форме практической подготовки**
Учебные занятия	434	242
Курсовая работа (проект)	-	-
Самостоятельная работа	64	
Практика, в т.ч.:	204	204
учебная	*84*	*84*
производственная	*120*	*120*
Промежуточная аттестация, в том числе: *МДК 01.01 в форме экзамена* *МДК 01.02. в форме экзамена* *МДК 01.05. в форме экзамена* *ПМ 01*	 6 6 6 12	
Всего	**732**	**446**

2.2. Структура профессионального модуля

Код ОК, ПК	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Обучение по МДК, в т.ч.:	Учебные занятия	Курсовая работа (проект)	Самостоятельная работа	Промежуточная аттестация	Учебная практика	Производственная практика
1	2	3	4	5	6	7	8		9	10
ОК 05; ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5	**Раздел 1** Операционные системы	**122**	**64**	**122**	100	-	16	6		
ОК 05; ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5	**Раздел 2** Базы данных	**102**	**48**	**102**	84	-	12	6		
ОК 05; ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5	**Раздел 3** Сети и системы передачи информации	**74**	**32**	**74**	64	-	10			
ОК 05; ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5	**Раздел 4** Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**98**	**42**	**98**	84	-	14			
ОК 05; ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5	**Раздел 5** Эксплуатация компьютерных сетей	**120**	**56**	**120**	102	-	12	6		
	Учебная практика	**84**	**84**						**84**	
	Производственная практика	**120**	**120**							**120**
	Промежуточная аттестация	**12**						*12*		
	Всего:	**732**	**446**	**516**	***434***	**-**	***64***	***30***	**84**	**120**

2.3. Содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК
1	2	3	4
Раздел 1 модуля. Операционные системы		**118/48**	
МДК.01.01		**118/48**	
Тема 1.1. Основы теории операционных систем	**Содержание**	**10**	
	Определение операционной системы. Основные понятия. История развития операционных систем.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Виды операционных систем. Классификация операционных систем по разным признакам.	2	
	Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы.	2	
	В том числе практических занятий и лабораторных работ	**2**	
	Исследование процесса загрузки ОС	2	
	В том числе самостоятельная работа обучающихся Исследования в области операционных систем.	2	
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	**Содержание**	**16**	
	Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Переносимость ОС. Машинно-зависимые модули ОС.	2	
	Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.	2	
	Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.	2	
	В том числе практических занятий и лабораторных работ	**8**	
	Виртуальные машины. Создание, модификация, работа	2	
	Установка ОС	2	
	Создание и изучение структуры разделов жесткого диска	2	
	Операции с файлами	2	
Тема 1.3. Модульная структура операционных систем, пространство пользователя	**Содержание**	**6**	
	Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**4**	

	Настройка параметров рабочей среды пользователя	2	
	Изучение основных команд для работы с файловой системой в консольном режиме	2	
Тема 1.4. Управление памятью	**Содержание**	**6**	
	Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти	2	
	В том числе практических занятий и лабораторных работ	**2**	
	Мониторинг за использованием памяти	2	
Тема 1.5. Управление процессами, многопроцессорные системы	**Содержание**	**8**	
	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	2	
	В том числе практических занятий и лабораторных работ	**4**	
	Управление процессами	2	
	Наблюдение за использованием ресурсов системы	2	
Тема 1.6. Виртуализация и облачные технологии	**Содержание**	**12**	
	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Виртуальные устройства. Вопросы лицензирования	2	
	Облачные технологии.	2	
	В том числе практических занятий и лабораторных работ	**2**	
	Изучение примеров виртуальных машин (VMware, VBox)	2	
	В том числе самостоятельная работа обучающихся Создание виртуальной машины Исследования в области виртуализации и облаков	2	
Тема 1.7. Принципы построения защиты информации в операционных системах	**Содержание**	**16**	
	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Порядок обеспечения безопасности информации при эксплуатации операционных систем. Штатные средства ОС для защиты информации.	2	
	Аутентификация, авторизация, аудит.	2	
	В том числе практических занятий и лабораторных работ	**8**	
	Управление учетными записями пользователей и доступом к ресурсам	2	

	Аудит событий системы	2	
	Изучение штатных средств защиты информации в операционных системах	4	
	В том числе самостоятельная работа обучающихся Анализ журнала аудита ОС	2	
Тема 1.8. Операционные системы UNIX, Linux и MacOS, Android	**Содержание**	**20**	
	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Операционные системы семейства Mac OS: особенности, преимущества и недостатки.	2	
	Операционные системы отечественных компаний: Astra Linux, Ред ОС.	2	
	Архитектура Android. Приложения Android	2	
	В том числе практических занятий и лабораторных работ	**8**	
	Создание дистрибутива Linux. Установка.	2	
	Работа в ОС Linux.	2	
	Установка и настройка отечественной ОС.	2	
	Настройка Android	2	
	В том числе самостоятельная работа обучающихся Анализ возможностей отечественных операционных систем	2	
Тема 1.9. Операционная система Windows	**Содержание**	**4**	
	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Установка и первичная настройка Windows.	2	
Тема 1.10. Серверные операционные системы	**Содержание**	**14**	
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**8**	
	Работа с сетевой файловой системой.	4	
	Работа с серверной ОС, например, AltLinux.	4	
	В том числе самостоятельная работа обучающихся Изучение аналитических обзоров в области построения систем безопасности операционных систем	4	
Обобщение тем МДК		**4**	
Промежуточная аттестация по МДК.01.01		**6**	
Раздел 2. Базы данных		**106/48**	
МДК.01.02 Базы данных		**106/48**	
	Содержание	**4**	

Тема 2.1. Основные понятия теории баз данных. Модели данных	Понятие базы данных. Компоненты системы БД: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Модели данных. Иерархические, сетевые и реляционные модели организации данных. Терминология реляционных моделей. Классификация сущностей.		
	В том числе самостоятельная работа обучающихся Централизованное управление данными, основные требования. Постреляционные модели данных. Двенадцать правил Кодда для определения концепции реляционной модели.	2	
Тема 2.2. Основы реляционной алгебры	**Содержание**	**4**	
	Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Традиционные операции над отношениями	2	
	Специальные операции над отношениями		
Тема 2.3. Базовые понятия и классификация систем управления базами данных	**Содержание**	**2**	
	Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Знакомство с СУБД SQL Server Management Studio		
Тема 2.4. Целостность данных как ключевое понятие баз данных	**Содержание**	**2**	
	В том числе самостоятельная работа обучающихся Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
Тема 2.5. Информационные модели реляционных баз данных	**Содержание**	**4**	
	Типы информационных моделей. Логические модели данных. Физические модели данных.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Проектирование инфологической модели данных	2	
Тема 2.6. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	**Содержание**	**8**	
	Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**4**	
	Проектирование структуры базы данных	2	
	Приведение таблицы к первой, второй и третьей нормальным формам.	2	

	В том числе самостоятельная работа обучающихся Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.	2	
Тема 2.7. Средства автоматизации проектирования	**Содержание**	**8**	
	CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**6**	
	Проектирование базы данных с использованием CASE-средств – диаграмма сущность-связь	2	
	Проектирование диаграммы потоков данных	2	
	Проектирование диаграммы прецедентов использования.	2	
Тема 2.8. Создание базы данных. Манипулирование данными.	**Содержание**	**6**	
	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. Команды хранения, добавления, редактирования, удаления и восстановления данных.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	2	
	В том числе самостоятельная работа обучающихся Открытие и модификация данных. Навигация по набору данных.	2	
Тема 2.9. Индексы. Связи между таблицами. Объединение таблиц	**Содержание**	**6**	
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**4**	
	Создание взаимосвязей	2	
	Сортировка, поиск и фильтрация данных Способы объединения таблиц	2	
Тема 2.10. Структурированный язык запросов SQL	**Содержание**	**4**	
	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	

	Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL	2	
Тема 2.11. Операторы и функции языка SQL	**Содержание**	**8**	
	Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**6**	
	Создание и использование запросов	2	
	Группировка и агрегирование данных		
	Коррелированные вложенные запросы	2	
	Создание в запросах вычисляемых полей. Использование условий	2	
Тема 2.12. Архитектуры распределенных баз данных	**Содержание**	**6**	
	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.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Управление доступом к объектам базы данных	2	
	В том числе самостоятельная работа обучающихся Отличия и преимущества удаленных баз данных от локальных баз данных. Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.	2	
Тема 2.13. Серверная часть распределенной базы данных	**Содержание**	**4**	
	Планирование и развёртывание СУБД для работы с клиентскими приложениями	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Установка СУБД. Настройка компонентов СУБД.	2	
Тема 2.14. Клиентская часть распределенной базы данных	**Содержание**	**10**	
	Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**6**	
	Создание форм. Создание отчетов	2	
	Создание меню. Генерация, запуск.	2	
	Профилирование запросов клиентских приложений.	2	
	В том числе самостоятельная работа обучающихся	2	

	Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа.		
Тема 2.15. Обеспечение целостности, достоверности и непротиворечивости данных.	**Содержание**	**6**	
	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.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**4**	
	Разработка хранимых процедур	2	
	Разработка триггеров. Создание представлений	2	
Тема 2.16. Перехват исключительных ситуаций и обработка ошибок	**Содержание**	**2**	
	В том числе самостоятельная работа обучающихся Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
Тема 2.17. Механизмы защиты информации в системах управления базами данных	**Содержание**	**4**	
	Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Управление правами доступа к базам данных. Средства защиты информации в базах данных	2	
Тема 2.18. Копирование и перенос данных. Восстановление данных	**Содержание**	**8**	
	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.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**4**	
	Аудит данных с помощью средств СУБД и триггеров	2	
	Резервное копирование и восстановление баз данных	2	
	В том числе самостоятельная работа обучающихся Автоматизация процессов копирования. Восстановление данных	2	
Обобщение тем МДК		**4**	

Промежуточная аттестация по МДК.01.02		**6**	
Раздел 3. Сети и системы передачи информации		**74/32**	
МДК.01.03 Сети и системы передачи информации		**74/32**	
Тема 3.1. Основные понятия и определения	**Содержание**	**12**	
	Классификация систем связи. Сообщения и сигналы.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Виды электронных сигналов. Спектральное представление сигналов.	2	
	Параметры сигналов. Объем и информационная емкость сигнала.	2	
	В том числе практических занятий и лабораторных работ	**6**	
	Особенности распространения ЭМВ, применение ЭМВ	2	
	Изучение и расчет параметров сигнала	2	
	Изучение видов модуляции сигналов	2	
Тема 3.2. Принципы передачи информации в сетях и системах связи	**Содержание**	**12**	
	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	2	
	В том числе практических занятий и лабораторных работ	**4**	
	Изучение принципов построения телекоммуникационных сетей	4	
	В том числе самостоятельная работа обучающихся Семиуровневая модель osi	4	
Тема 3.3. Типовые каналы передачи и их характеристики	**Содержание**	**10**	
	Канал передачи. Сетевой тракт, групповой канал передачи.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Аппаратура цифровых плезиохронных систем передачи.	2	
	Основные параметры и характеристики сигналов.	2	
	В том числе практических занятий и лабораторных работ	**2**	
	Расчет пропускной способности канала связи	2	
	В том числе самостоятельная работа обучающихся Упрощённая схема организации канала	2	
Тема 3.4. Архитектура и принципы работы современных сетей передачи данных	**Содержание**	**22**	
	Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Маршрутизация и управление потоками в сетях связи.	2	
	Протоколы и интерфейсы управления каналами и сетью передачи данных.	2	
	В том числе практических занятий и лабораторных работ	**14**	
	Изучение структуры стандартов	2	

	Конфигурирование сетевого интерфейса рабочей станции	2	
	Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP	2	
	Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне	2	
	Диагностика и разрешение проблем сетевого уровня	2	
	Диагностика и разрешение проблем протоколов транспортного уровня	2	
	Диагностика и разрешение проблем протоколов прикладного уровня	2	
	В том числе самостоятельная работа обучающихся Переадресация пакетов	2	
Тема 3.5. Беспроводные системы передачи данных	**Содержание**	**6**	
	Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	2	
	В том числе практических занятий и лабораторных работ	**2**	
	Настройка Wi-Fi маршрутизатора	2	
Тема 3.6. Сотовые и спутниковые системы	**Содержание**	**10**	
	Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA.	2	
	Спутниковые системы передачи данных.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**4**	
	Устройства сотовой связи	2	
	Устройства спутниковой связи	2	
	В том числе самостоятельная работа обучающихся Современные беспроводные системы	2	
Промежуточная аттестация по МДК.01.03 (дифзачет)		**2**	
Раздел 4. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**98/42**	
МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**98/42**	
Тема 4.1. Основы информационных систем как объекта защиты.	**Содержание**	**6**	
	Понятие автоматизированной (информационной) системы. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.		
	В том числе практических занятий и лабораторных работ	**2**	

	Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	2	
	В том числе самостоятельная работа обучающихся Примеры областей применения АИС. Основные особенности современных проектов АИС. Электронный документооборот	2	
Тема 4.2. Жизненный цикл автоматизированных систем	**Содержание**	**10**	
	Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Требования к автоматизированной системе в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.	2	
	В том числе практических занятий и лабораторных работ	**2**	
	Задачи и этапы проектирования АС в защищенном исполнении. Разработка технического задания на проектирование автоматизированной системы	2	
	В том числе самостоятельная работа обучающихся Методологии проектирования. Организация работ, функции заказчиков и разработчиков. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении.	2	
Тема 4.3. Угрозы безопасности информации в автоматизированных системах	**Содержание**	**8**	
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Методы оценки опасности угроз. Банк данных угроз безопасности информации Понятие уязвимости угрозы. Классификация уязвимостей.	2	
	В том числе практических занятий и лабораторных работ	**4**	
	Категорирование информационных ресурсов.	2	
	Анализ угроз безопасности информации. Построение модели угроз	2	
Тема 4.4. Основные меры защиты информации в автоматизированных системах	**Содержание**	**4**	
	В том числе практических занятий и лабораторных работ	**2**	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Изучение нормативно-правовой базы для определения мер защиты информации в автоматизированных информационных системах и требований к ним	2	
	В том числе самостоятельная работа обучающихся	**2**	

	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.		
Тема 4.5. Содержание и порядок эксплуатации АС в защищенном исполнении	**Содержание**	**12**	
	Защита машинных носителей информации. Регистрация событий безопасности Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации	2	
	Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных. Резервное копирование и восстановление данных.	2	
	В том числе практических занятий и лабораторных работ	**6**	
	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	2	
	Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	2	
	Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ. Обнаружение (предотвращение) вторжений	2	
	В том числе самостоятельная работа обучающихся Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.	2	
Тема 4.6. Защита информации в распределенных автоматизированных системах	**Содержание**	**4**	
	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
Тема 4.7. Особенности разработки информационных систем персональных данных	**Содержание**	**4**	
	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Определения уровня защищенности ИСПДн. Выбор мер по обеспечению безопасности ПДн	2	

Тема 4.8. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	**Содержание**	**6**	
	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.		
	В том числе практических занятий и лабораторных работ	**2**	
	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Мониторинг и аудит, выявление угроз информационной безопасности автоматизированных систем	2	
	В том числе самостоятельная работа обучающихся Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	2	
Тема 4.9. Администрирование автоматизированных систем	**Содержание**	**4**	
	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Управление, тестирование и эксплуатация автоматизированных систем	2	
Тема 4.10. 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.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
Тема 4.11. Защита от несанкционированного доступа к информации	**Содержание**	**6**	
	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Требования защищенности СВТ от НСД к информации Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	2	
	В том числе практических занятий и лабораторных работ	**2**	
	Классификация автоматизированных систем. Требования по защите информации от НСД для АС	2	

Тема 4.12. СЗИ от НСД	**Содержание**	**20**	
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.	2	
	Обеспечение целостности информационной системы и информации	2	
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности		
	В том числе практических занятий и лабораторных работ	**12**	
	Установка и настройка СЗИ от НСД Защита входа в систему (идентификация и аутентификация пользователей)	2	
	Разграничение доступа к устройствам. Управление доступом. Управление грифами конфиденциальности.	2	
	Управление доступом и контроль печати конфиденциальной информации. Настройка механизма полномочного управления доступом. Использование принтеров для печати конфиденциальных документов. Контроль печати	2	
	Настройка регистрации событий. Управление режимом потоков.	2	
	Настройка системы для задач аудита.	2	
	Настройка контроля целостности и замкнутой программной среды. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	2	
	В том числе самостоятельная работа обучающихся Общие принципы управления. Основные механизмы защиты. Правила работы с конфиденциальными ресурсами.	2	
Тема 4.13. Эксплуатация средств защиты информации в компьютерных сетях	**Содержание**	**8**	
	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении		
	В том числе практических занятий и лабораторных работ	**4**	
	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	2	
	Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	2	

	В том числе самостоятельная работа обучающихся Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	2	
Тема 4.14. Документация на защищаемую автоматизированную систему	**Содержание**	**4**	
	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Оформление основных эксплуатационных документов на автоматизированную систему.	2	
Промежуточная аттестация по МДК.01.04 **дифференцированный зачет**		**2**	
Раздел 5 Эксплуатация компьютерных сетей		**120/56**	
МДК.01.05. Эксплуатация компьютерных сетей		**120/56**	
Тема 5.1. Модели сетевого взаимодействия	**Содержание**	**4**	
	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.		
	В том числе практических занятий и лабораторных работ	**2**	
	Изучение элементов кабельной системы.	2	
Тема 5.2. Физический уровень модели OSI	**Содержание**	**6**	
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Стандарты кабелей. Электрическая проводка. Оптоволоконные линии связи		
	В том числе практических занятий и лабораторных работ	**2**	
	Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	2	
	В том числе самостоятельная работа обучающихся Беспроводная среда передачи	**2**	
Тема 5.3. Топология компьютерных сетей	**Содержание**	**6**	
	Понятие топологии сети. Обзор сетевых топологий**.**	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Сетевое оборудование в топологии.		
	В том числе практических занятий и лабораторных работ	**4**	

	Построение одноранговой сети	2	
	Разработка топологи сети небольшого предприятия	2	
Тема 5.4. Технологии Ethernet	**Содержание**	**4**	
	Обзор технологий построения локальных сетей. Технология Ethernet.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Изучение адресации канального уровня. MAC-адреса.	2	
Тема 5.5. Технологии коммутации	**Содержание**	**6**	
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI. Конструктивное исполнение коммутаторов	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Создание коммутируемой сети	2	
	В том числе самостоятельная работа обучающихся Программное обеспечение коммутаторов. Общие принципы сетевого дизайна	**2**	
Тема 5.6. Сетевой протокол IPv4	**Содержание**	**6**	
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Маршрутизация пакетов IPv4. Протоколы динамической маршрутизации	2	
	В том числе практических занятий и лабораторных работ	**2**	
	Изучение IP-адресации.	2	
Тема 5.7. Скоростные и беспроводные сети	**Содержание**	**4**	
	Сеть FDDI. Сеть 100VG-AnyLAN. Сверхвысокоскоростные сети. Беспроводные сети	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Настройка беспроводного сетевого оборудования	2	
Тема 5.8. Основы коммутации	**Содержание**	**6**	
	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Работа с основными командами коммутатора.	2	
	В том числе самостоятельная работа обучающихся Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов	**2**	

Тема 5.9. Начальная настройка коммутатора	**Содержание**	**8**	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.	2	
	Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор.		
	В том числе практических занятий и лабораторных работ	**4**	
	Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов.	2	
	Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	2	
	В том числе самостоятельная работа обучающихся Загрузка и резервное копирование конфигурации коммутатора.	**2**	
Тема 5.10. Виртуальные локальные сети (VLAN)	**Содержание**	**8**	
	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**6**	
	Настройка VLAN на основе стандарта IEEE 802.1Q.	2	
	Настройка протокола GVRP.	2	
	Настройка сегментации трафика без использования VLAN.	2	
Тема 5.11. Функции повышения надежности и производительности	**Содержание**	**6**	
	Протокол Spanning Tree Protocol (STP). Уязвимостипротокола STP.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Дополнительные функции защиты от петель. Агрегирование каналов связи.		
	В том числе практических занятий и лабораторных работ	**4**	
	Настройка протоколов связующего дерева STP, RSTP, MSTP.	2	
	Настройка функции защиты от образования петель LoopBackDetection. Агрегирование каналов.	2	
Тема 5.12. Адресация сетевого уровня и маршрутизация	**Содержание**	**10**	
	Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP. Протокол NDP.		
	В том числе практических занятий и лабораторных работ	**8**	
	Основные и расширенные конфигурации маршрутизатора.	2	
	Работа с протоколом CDP. Работа с протоколом TELNET. Работа с протоколом TFTP.	2	
	Работа с протоколом RIP и OSPF.	2	

	Конфигурирование функции маршрутизатора NAT/PAT. Конфигурирование PPP и CHAP.	2	
Тема 5.13. Качество обслуживания (QoS)	**Содержание**	**4**	
	Модели QoS. Приоритезация пакетов. Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Настройка QoS. Приоритезация трафика. Управление полосой пропускания	2	
Тема 5.14. Функции обеспечения безопасности и ограничения доступа к сети	**Содержание**	**6**	
	Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**4**	
	Списки управления доступом (AccessControlList). Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.	2	
	Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	2	
Тема 5.15. Многоадресная рассылка	**Содержание**	**4**	
	Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Отслеживание трафика многоадресной рассылки. Отслеживание трафика Multicast.	2	
Тема 5.16. Функции управления коммутаторами	**Содержание**	**4**	
	Управление множеством коммутаторов. Протокол SNMP. RMON (Remote Monitoring). Функция Port Mirroring.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Функции анализа сетевого трафика. Настройка протокола управления топологией сети LLDP.	2	
Тема 5.17. 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	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
Тема 5.18. Межсетевые экраны	**Содержание**	**6**	
	Технологии межсетевых экранов. Политика межсетевого экрана.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Межсетевые экраны с возможностями NAT.		
	Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.		
	В том числе практических занятий и лабораторных работ	**2**	

	Основы администрирования межсетевого экрана. Создание политик для традиционного (или исходящего) NAT.	2	
	В том числе самостоятельная работа обучающихся Соединение двух локальных сетей межсетевыми экранами. Создание политики без проверки состояния.	**2**	
Тема 5.19. Системы обнаружения и предотвращения проникновений	**Содержание**	**6**	
	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	Требования организации к функционированию IDPS. Развертывание IDPS.		
	В том числе практических занятий и лабораторных работ	**4**	
	Обнаружение и предотвращение вторжений.	2	
	Возможности IDPS. Сильные стороны и ограниченность IDPS.	2	
Тема 5.20. Приоритизация трафика и создание альтернативных маршрутов	**Содержание**	**4**	
	Создание альтернативных маршрутов доступа в Интернет. Приоритизация трафика.	2	ОК 05 ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4
	В том числе практических занятий и лабораторных работ	**2**	
	Создание альтернативных маршрутов с использованием статической маршрутизации	2	
Обобщение разделов МДК.01.05		**4**	
Промежуточная аттестация по МДК.01.05		**6**	
– **Учебная практика** – **Виды работ:** – установка программного обеспечения в соответствии с технической документацией. – настройка параметров работы программного обеспечения, включая системы управления базами данных. – настройка компонентов подсистем защиты информации операционных систем. – управление учетными записями пользователей. – работа в операционных системах с соблюдением действующих требований по защите информации. – установка обновления программного обеспечения. – контроль целостность подсистем защиты информации операционных систем. – выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных – использование программных средств для архивирования информации. – проведение аудита защищенности автоматизированной системы. – установка, настройка и эксплуатация сетевых операционных систем. – диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.		***84***	

– организация работ с удаленными хранилищами данных и базами данных. – организация защищенной передачи данных в компьютерных сетях. – выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. – осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. – заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.		
Производственная практика **Виды работ:** – участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации – обслуживание средств защиты информации прикладного и системного программного обеспечения – настройка программного обеспечения с соблюдением требований по защите информации – настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам – настройка встроенных средств защиты информации программного обеспечения – проверка функционирования встроенных средств защиты информации программного обеспечения – своевременное обнаружение признаков наличия вредоносного программного обеспечения – обслуживание средств защиты информации в компьютерных системах и сетях – обслуживание систем защиты информации в автоматизированных системах – участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем – проверка работоспособности системы защиты информации автоматизированной системы – контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации – контроль стабильности характеристик системы защиты информации автоматизированной системы – ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем – участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	***120***	
Экзамен по профессиональному модулю	**12**	
Всего	**732/430**	

2.4. Курсовая работа Выполнение курсовой работы не предусмотрено

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Мастерская «Кибербезопасности», оснащенная в соответствии с приложением 3 ОПОП-П. . с п. 3.1.2. образовательной программы

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

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2018.

2. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2019

3. 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. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/153938 — Режим доступа: для авториз. пользователей.

4. 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. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176902 — Режим доступа: для авториз. пользователей.

5. Соснин, П. И. Архитектурное моделирование автоматизированных систем : учебник для спо / П. И. Соснин. — 3-е изд., стер. — Санкт-Петербург : Лань, 2023. — 180 с. — ISBN 978-5-507-46075-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/297017 — Режим доступа: для авториз. пользователей.

6. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для спо / А. Г. Уймин. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 480 с. — ISBN 978-5-8114-9255-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189420 — Режим доступа: для авториз. пользователей.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код ПК, ОК	Критерии оценки результата (показатели освоенности компетенций)	Формы контроля и методы оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрирует умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявляет умения и практический опыт администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проводит перечень работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявляет знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Грамотно владеет устной и письменной речью Ясно формулирует и излагает мысли	

Приложение 1.2
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа профессионального модуля

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

2024 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «защита информации в автоматизированных системах программными и программно-аппаратными средствами».

Профессиональный модуль включен в обязательную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.2. Планируемые результаты освоения профессионального модуля

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

результате освоения профессионального модуля обучающийся должен:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК 08	– использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей – применять рациональные приемы двигательных функций в профессиональной деятельности – пользоваться средствами профилактики перенапряжения, характерными для данной специальности	– роль физической культуры в общекультурном, профессиональном и социальном развитии человека – основы здорового образа жизни – условия профессиональной деятельности и зоны риска физического здоровья для специальности – средства профилактики перенапряжения	
ПК 2.1.	– устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации	– особенности и способы применения программных и программно- аппаратных средств защиты информации, в том числе, в операционных системах, Компьютерных сетях, базах данных	– выполнять установку, настройку программных средств защиты информации в автоматизированной
ПК 2.2.	– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	– особенности и способы применения программных и программно- аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	– обеспечивать защиту автономных автоматизированных систем программными и программно-аппаратными средствами – использовать программные и программно-аппаратные средства для защиты информации в сети

ПК 2.3.	– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	– тестировать функций, диагностировать работоспособности программных и программно-аппаратных средств защиты информации – устранять отказы и восстанавливать работоспособности программных и программно-аппаратных средств защиты информации
ПК 2.4.	– 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	– особенности и способы применения программных и программно- аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации – основные понятия криптографии и типовых криптографических методов и Средств защиты информации	– решать задачи защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации – применять электронную подпись, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных
ПК 2.5.	– применять средства гарантированного уничтожения информации	– особенности и способы применения программных уничтожения информации – особенности и способы применения программно-аппаратных средств гарантированного уничтожения информации	– учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности
ПК 2.6	– 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	– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	– выполнять работу с подсистемами регистрации событий – выявлять события и инцидентов безопасности в автоматизированной системе

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Трудоемкость освоения модуля

Наименование составных частей модуля	**Объем в часах**	**В т.ч. в форме практической подготовки**
Учебные занятия	258	126
Курсовая работа (проект)	20	20
Самостоятельная работа	48	
Практика, в т.ч.:	204	204
учебная	*48*	*48*
производственная	*156*	*156*
Промежуточная аттестация, в том числе: *МДК 02.01 в форме экзамена* *МДК 02.02. в форме экзамена* *ПМ 02*	 12 6 12	
Всего	**560**	**352**

2.2. Структура профессионального модуля

Код ОК, ПК	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Обучение по МДК, в т.ч.:	Учебные занятия	Курсовая работа (проект)	Самостоятельная работа	Промежуточная аттестация	Учебная практика	Производственная практика
1	2	3	4	5	6	7	8		9	10
ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5 ПК 2.6	**Раздел 1** Программные и программно-аппаратные средства защиты информации	**198**	**84**	**198**	142	20	24	12		
ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5 ПК 2.6	**Раздел 2** Криптографические средства защиты информации	**146**	**62**	**146**	116		24	6		
	Учебная практика	**48**	**48**						**48**	
	Производственная практика	**156**	**156**							**156**
	Промежуточная аттестация	**12**								
	Всего:	**560**	**350**	**344**	***258***	***20***	***48***	***18***	**48**	**156**

2.3. Содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Код ПК, ОК
1	2		
Раздел 1 Программные и программно-аппаратные средства защиты информации		**198/84**	
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**198/84**	
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**	**2**	
	Предмет и задачи программно-аппаратной защиты информации	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Основные понятия программно-аппаратной защиты информации		
	Классификация методов и средств программно-аппаратной защиты информации		
Тема 1.2. Стандарты безопасности	**Содержание**	**6**	
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	В том числе практических и лабораторных занятий	**2**	
	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.	2	
	В том числе самостоятельная работа обучающихся Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	**2**	
	Содержание	**22**	

Тема 1.3. Защищенная автоматизированная система	Автоматизация процесса обработки информации	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Понятие автоматизированной системы.		
	Особенности автоматизированных систем в защищенном исполнении.	2	
	Основные виды АС в защищенном исполнении.		
	Дискреционные модели	2	
	Мандатные модели		
	В том числе практических и лабораторных занятий	**14**	
	Учет, обработка, хранение и передача информации в АИС	2	
	Ограничение доступа на вход в систему. Разграничение доступа.	2	
	Идентификация и аутентификация пользователей	2	
	Регистрация событий (аудит).	2	
	Контроль целостности данных. Уничтожение остаточной информации.	2	
	Управление политикой безопасности. Шаблоны безопасности	2	
	Криптографическая защита. Обзор программ шифрования данных	2	
	В том числе самостоятельная работа обучающихся Методы создания безопасных систем Методология проектирования гарантированно защищенных КС	**2**	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**	**6**	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Источники дестабилизирующего воздействия на объекты защиты	2	
	Способы воздействия на информацию		
	В том числе практических и лабораторных занятий	**2**	
	Распределение каналов в соответствии с источниками воздействия на информацию	2	
	В том числе самостоятельная работа обучающихся Причины и условия дестабилизирующего воздействия на информацию	**2**	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**	**10**	
	Понятие несанкционированного доступа к информации	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Основные подходы к защите информации от НСД		
	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	2	
	Доступ к данным со стороны процесса		

	В том числе практических и лабораторных занятий	**4**	
	Организация доступа к файлам	2	
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	2	
	В том числе самостоятельная работа обучающихся Особенности защиты данных от изменения. Шифрование	**2**	
Тема 1.6 Основы защиты автономных автоматизированных систем	**Содержание**	**6**	
	Работа автономной АС в защищенном режиме	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	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)	2	
	В том числе самостоятельная работа обучающихся Применение закладок, направленных на снижение эффективности средств, замыкающих среду	**2**	
Тема 1.7 Защита программ от изучения	**Содержание**	**6**	
	Изучение и обратное проектирование ПО	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Способы изучения ПО: статическое и динамическое изучение		
	Задачи защиты от изучения и способы их решения	2	
	В том числе самостоятельная работа обучающихся Защита от отладки. Защита от дизассемблирования Защита от трассировки по прерываниям	**2**	
Тема 1.8 Вредоносное программное обеспечение	**Содержание**	**8**	
	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Бот-неты. Принцип функционирования. Методы обнаружения	2	
	Классификация антивирусных средств. Сигнатурный и эвристический анализ		
	В том числе практических и лабораторных занятий	**2**	

	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО Основные концепции построения систем антивирусной защиты на предприятии	2	
	В том числе самостоятельная работа обучающихся Вредоносное программное обеспечение как особый вид разрушающих воздействий. Поиск следов активности вредоносного ПО. Реестр Windows. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. Основные ветки, содержащие информацию о вредоносном ПО. Защита от вирусов в "ручном режиме"	**2**	
Тема 1.9 Защита программ и данных от несанкционированного копирования	**Содержание**	**7**	
	Несанкционированное копирование программ как тип НСД	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Привязка ПО к аппаратному окружению и носителям.		
	Защитные механизмы в современном программном обеспечении на примере MS Office		
	В том числе практических и лабораторных занятий	**4**	
	Защита информации от несанкционированного копирования с использованием специализированных программных средств	2	
	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	2	
	В том числе самостоятельная работа обучающихся Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования	**1**	
Тема 1.10 Защита информации на машинных носителях	**Содержание**	**14**	
	Проблема защиты отчуждаемых компонентов ПЭВМ.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Методы защиты информации на отчуждаемых носителях. Шифрование.		
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	2	
	Безвозвратное удаление данных. Принципы и алгоритмы.		
	В том числе практических и лабораторных занятий	**8**	
	Применение средства восстановления остаточной информации на примере Foremost или аналога	2	

	Применение специализированного программного средства для восстановления удаленных файлов	2	
	Применение программ для безвозвратного удаления данных	2	
	Применение программ для шифрования данных на съемных носителях	2	
	В том числе самостоятельная работа обучающихся Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	**2**	
Тема 1.11 Аппаратные средства идентификации и аутентификации пользователей	**Содержание**	**2**	
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Устройства Touch Memory		
Тема 1.12. Системы обнаружения атак и вторжений	**Содержание**	**8**	
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Использование сетевых снифферов в качестве СОВ		
	Аппаратный компонент СОВ	2	
	Программный компонент СОВ		
	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений.		
	В том числе практических и лабораторных занятий	**2**	
	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2	
	В том числе самостоятельная работа обучающихся Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	**2**	
Тема 1.13 Основы построения защищенных сетей	**Содержание**	**4**	
	Сети, работающие по технологии коммутации пакетов	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Стек протоколов TCP/IP. Особенности маршрутизации.		
	Штатные средства защиты информации стека протоколов TCP/IP.	2	
	Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.		

Тема 1.14 Средства организации VPN	**Содержание**	**6**	
	Виртуальная частная сеть. Функции, назначение, принцип построения	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Криптографические и некриптографические средства организации VPN		
	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	2	
	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки		
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки		
	В том числе практических и лабораторных занятий	**2**	
	Развертывание VPN	2	
Тема 1.15 Обеспечение безопасности межсетевого взаимодействия	**Содержание**	**10**	
	Методы защиты информации при работе в сетях общего доступа.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности		
	Основные типы firewall. Симметричные и несимметричные firewall.		
	Уровень 1. Пакетные фильтры	2	
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.		
	Уровень 3. Proxy-сервера прикладного уровня		
	В том числе практических и лабораторных занятий	**4**	
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	2	
	Изучение различных способов закрытия "опасных" портов	2	
	В том числе самостоятельная работа обучающихся Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций Требования по сертификации межсетевых экранов	**2**	
Тема 1.16 Защита информации в базах данных	**Содержание**	**8**	
	Основные типы угроз. Модель нарушителя	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6**.**
	Средства идентификации и аутентификации. Управление доступом		
	Средства контроля целостности информации в базах данных		

	В том числе практических и лабораторных занятий	**4**	
	Изучение механизмов защиты СУБД MS Access	2	
	Изучение штатных средств защиты СУБД MSSQL Server	2	
	В том числе самостоятельная работа обучающихся Средства аудита и контроля безопасности. Критерии защищенности баз данных. Применение криптографических средств защиты информации в базах данных	**2**	
Тема 1.17 Мониторинг систем защиты	**Содержание**	**9**	
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	2	
	Классификация отслеживаемых событий. Особенности построения систем мониторинга		
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	2	
	Классификация сетевых мониторов		
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.		
	В том числе практических и лабораторных занятий	**4**	
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	2	
	Проведение аудита ЛВС сетевым сканером	2	
	В том числе самостоятельная работа обучающихся Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	**1**	
Тема 1.18 Изучение мер защиты информации в информационных системах	**Содержание**	**2**	
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.		ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	В том числе практических и лабораторных занятий	**2**	
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	2	

Тема 1.19 Изучение современных программно-аппаратных комплексов.	**В том числе практических и лабораторных занятий**	**10**	
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	2	
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов	2	
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов	2	
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	2	
Курсовая работа		**20**	
Промежуточная аттестация по МДК.02.01	**экзамен 3 семестр**	**6**	
Промежуточная аттестация по МДК.02.01	**экзамен 4 семестр**	**6**	
Раздел 2. Криптографические средства защиты информации		**146/62**	
МДК.02.02. Криптографические средства защиты информации		**146/62**	
Тема 2.1. Математические основы криптографии	**Содержание**	**22**	
	Элементы теории множеств. Группы, кольца, поля.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Делимость чисел. Признаки делимости. Простые и составные числа.	2	
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.		
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	2	
	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.		
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	2	
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	2	

	В том числе практических и лабораторных занятий	**6**	
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	2	
	Проверка чисел на простоту	2	
	Решение задач с элементами теории чисел.	2	
	В том числе самостоятельная работа обучающихся История развития криптографии Китайская теорема об остатках. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра Арифметические операции над большими числами. Эллиптические кривые и их приложения в криптографии	**6**	
Тема 2.2. Методы криптографического защиты информации	**Содержание**	**16**	
	Классификация основных методов криптографической защиты. Методы симметричного шифрования	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2	
	Методы перестановки. Табличная перестановка, маршрутная перестановка	2	
	Гаммирование. Гаммирование с конечной и бесконечной гаммами	2	
	В том числе практических и лабораторных занятий	**8**	
	Применение классических шифров замены	2	
	Применение классических шифров перестановки	2	
	Применение метода гаммирования	2	
	Программная реализация классических шифров	2	
Тема 2.3. Криптоанализ	**Содержание**	**16**	
	Основные методы криптоанализа. Криптографические атаки.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	2	
	В том числе практических и лабораторных занятий	**10**	
	Криптоанализ шифра простой замены методом анализа частотности символов	2	
	Криптоанализ классических шифров методом полного перебора ключей	4	

	Криптоанализ шифра Вижинера	4	
	В том числе самостоятельная работа обучающихся Перспективные направления криптоанализа, квантовый криптоанализ Оптимизация методов частотного анализа моноалфавитных шифров	**2**	
Тема 2.4. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	**6**	
	Основные принципы поточного шифрования.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.		
	В том числе практических и лабораторных занятий	**2**	
	Применение методов генерации ПСЧ	2	
	В том числе самостоятельная работа обучающихся Применение генераторов ПСЧ в криптографии	**2**	
Тема 2.5 Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	**10**	
	Кодирование информации. Символьное кодирование. Смысловое кодирование.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств.		
	В том числе практических и лабораторных занятий	**6**	
	Кодирование информации	2	
	Программная реализация классических шифров	2	
	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	2	
	В том числе самостоятельная работа обучающихся Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII. Изучение современных программных и аппаратных криптографических средств	**2**	
Тема 2.6 Симметричные системы шифрования	**Содержание учебного материала**	**8**	
	Общие сведения. Структурная схема симметричных криптографических систем	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	2	
	В том числе практических и лабораторных занятий	**4**	

	Анализ современных симметричных криптоалгоритмов	2	
	Изучение программной реализации современных симметричных шифров	2	
Тема 2.7 Асимметричные системы шифрования	**Содержание учебного материала**	**10**	
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Элементы теории чисел в криптографии с открытым ключом.	2	
	В том числе практических и лабораторных занятий	**6**	
	Анализ современных асимметричных криптоалгоритмов	2	
	Применение различных асимметричных алгоритмов.	2	
	Изучение программной реализации асимметричного алгоритма RSA	2	
Тема 2.8 Аутентификация данных. Электронная подпись	**Содержание учебного материала**	**12**	
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Алгоритмы цифровой подписи	2	
	В том числе практических и лабораторных занятий	**8**	
	Применение различных функций хеширования, анализ особенностей хешей	2	
	Применение криптографических атак на хеш-функции.	2	
	Изучение программно-аппаратных средств, реализующих основные функции ЭП	4	
Тема 2.9 Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	**8**	
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем. Протоколы аутентификации.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	В том числе практических и лабораторных занятий	**4**	
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2	
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	2	
	В том числе самостоятельная работа обучающихся Взаимная аутентификация. Односторонняя аутентификация	**2**	
Тема 2.10	**Содержание учебного материала**	**4**	

Криптозащита информации в сетях передачи данных	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей.	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	2	
	В том числе самостоятельная работа обучающихся Криптомаршрутизатор. Пакетный фильтр	**2**	
Тема 2.11 Защита информации в электронных платежных системах	**Содержание учебного материала**	**8**	
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.		
	В том числе практических и лабораторных занятий	**4**	
	Применение аутентификации по одноразовым паролям.	2	
	Реализация алгоритмов создания одноразовых паролей	2	
	В том числе самостоятельная работа обучающихся Средства аутентификации в платежных системах	**2**	
Тема 2.12 Компьютерная стеганография	**Содержание учебного материала**	**8**	
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации	2	ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.
	Методы компьютерной стеганографии. Цифровые водяные знаки.		
	В том числе практических и лабораторных занятий	**4**	
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	2	
	Реализация простейших стеганографических алгоритмов	2	
	В том числе самостоятельная работа обучающихся Законодательство в области криптографической защиты информации Защита авторских прав. Алгоритмы встраивания ЦВЗ	**4**	
Обобщение разделов МДК		**4**	
Промежуточная аттестация по МДК.03.02	**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 − Применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных − Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	**48**	
Производственная практика **Виды работ:** −Участие в установке и настройку отдельных программных, программно-аппаратных средств защиты информации. − Участие в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. − Участие в тестировании функций отдельных программных и программно-аппаратных средств защиты информации. − Участие в обработке, хранении и передаче информации ограниченного доступа. − Участие в уничтожении информации и носителей информации с использованием программных и программно-аппаратных средств.	**156**	

− Участие в решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации − Осуществление регистрации основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. – 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. – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики		
Экзамен по профессиональному модулю	**12**	
Всего:	**560/350**	

2.4. Курсовая работа

Выполнение курсовой работы обязательно

Тематика курсовых работ:

– Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)

– Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)

– Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)

– Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)

– Проблема защиты информации в облачных хранилищах данных и ЦОДах

– Защита сред виртуализации

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Мастерская «Кибербезопасности», оснащенная(ые) в соответствии с приложением 3 ОПОП-П.

Оснащенные базы практики (мастерские/зоны по видам работ), оснащенная(ые) в соответствии с приложением 3 ОПОП-П. . с п. 3.1.2. образовательной программы.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2020.- 175 с.

2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2019.- 248 с.

3. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2020.- 400 с.

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, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт].

5. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт].

3.2.2 Дополнительные источники:

1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2019. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности

2. Федеральный образовательный портал «Информационно -коммуникационные технологии в образовании». [Электронный ресурс] – Режим доступа: http://window.edu.ru/resource/832/7832

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявляет знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.6. 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.	Проявляет знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	Выполняет правила ТБ во время учебных занятий, при прохождении учебной и производственной практик	

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

Рабочая программа профессионального модуля

«ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ»

2024 г.

СОДЕРЖАНИЕ

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

1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «защита информации техническими средствами».

Профессиональный модуль включен в обязательную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.3. Планируемые результаты освоения профессионального модуля

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

В результате освоения профессионального модуля обучающийся должен:

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
ОК.09	– понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы – участвовать в диалогах на знакомые общие и профессиональные темы – строить простые высказывания о себе и о своей профессиональной деятельности – кратко обосновывать и объяснять свои действия (текущие и планируемые) – писать простые связные сообщения на знакомые или интересующие профессиональные темы	– правила построения простых и сложных предложений на профессиональные темы – основные общеупотребительные глаголы (бытовая и профессиональная лексика) – лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности – особенности произношения – правила чтения текстов профессиональной направленности	-
ПК 3.1.	– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных	– порядок технического обслуживания технических средств защиты информации – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам	– установка, монтаж и настройка технических средств защиты информации – техническое обслуживание технических средств защиты информации – применение основных типов технических средств защиты информации

ПК 3.2.	– применять технические средства для криптографической защиты информации конфиденциального характера – применять технические средства для уничтожения информации и носителей информации – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами	– 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 применяемых средств защиты информации от несанкционированной утечки по техническим каналам	– применять основные типы технических средств защиты информации – выявлять технические каналы утечки информации – участвовать в мониторинге эффективности технических средств защиты информации – диагностировать, устранять отказы и неисправности, восстанавливать работоспособности технических средств защиты информации
ПК 3.3.	– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных	– номенклатуру и характеристики аппаратуры, используемой для измерения параметров пэмин, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации – структуру и условия формирования технических каналов утечки информации	– проводить измерения параметров пэмин, созданные техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации
ПК 3.4.	– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных	– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам	– проводить измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации – выявлять технические каналы утечки информации
ПК 3.5.	– основные принципы действия и характеристики технических средств физической защиты – основные способы физической защиты объектов информатизации – номенклатуру применяемых средств физической защиты объектов информатизации	– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом – применять инженерно-технические средства физической защиты объектов информатизации	– устанавливать, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей – восстанавливать работоспособности инженерно-технических средств физической защиты

1.4. Обоснование часов вариативной части ОПОП-П

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Трудоемкость освоения модуля

Наименование составных частей модуля	**Объем в часах**	**В т.ч. в форме практической подготовки**
Учебные занятия	262	116
Курсовая работа (проект)	20	20
Самостоятельная работа	42	
Практика, в т.ч.:	144	144
учебная	*36*	*36*
производственная	*108*	*108*
Промежуточная аттестация, в том числе: *МДК 03.01 в форме экзамена* *МДК 03.02. в форме экзамена* *ПМ 03*	 6 6 12	
Всего	**492**	**280**

2.2. Структура профессионального модуля

Код ОК, ПК	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Обучение по МДК, в т.ч.:	Учебные занятия	Курсовая работа (проект)	Самостоятельная работа	Промежуточная аттестация	Учебная практика	Производственная практика
1	2	3	4	5	6	7	8		9	10
ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5	**Раздел 1** Техническая защита информации	**172**	**64**	**172**	146	-	20	6		
ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5	**Раздел 2** Инженерно-технические средства физической защиты объектов информатизации	**164**	**72**	**164**	116	20	22	6		
	Учебная практика	**36**	**36**						**36**	
	Производственная практика	**108**	**108**							**108**
	Промежуточная аттестация	**12**								
	Всего:	**492**	**280**	**336**	***262***	***20***	***42***	***12***	**36**	**108**

2.3. Содержание профессионального модуля

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятия, курсовая работа (проект)	Объем, ак. ч. / в том числе в форме практической подготовки, ак. ч	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Техническая защита информации		**172**	
МДК.03.01 Техническая защита информации		**166**	
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**2**	
	Входной контроль. 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.	2	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**2**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Задачи и требования к способам и средствам защиты информации техническими средствами. Классификация способов и средств защиты информации.	2	
Тема 1.3. Информация как предмет защиты	**Содержание**	**8**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.	2	
	Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы.	2	
	Угрозы безопасности информации, факторы влияющие на возможность реализации угроз.	2	

	Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2	
	В том числе практических и лабораторных занятий	**8**	
	Изучение нормативной базы правового регулирования вопросов защиты информации	2	
	Анализ стандартов информационной безопасности по вопросам технической защиты информации	2	
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	2	
	Изучение демаскирующих признаков объектов защиты.	2	
Тема 1.4. Технические каналы утечки информации	**Содержание**	**8**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации.	2	
	Характеристика каналов утечки информации. Оптические каналы утечки информации, их характеристика.	2	
	Акустические, каналы утечки информации, их характеристика	2	
	Радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	2	
	В том числе практических и лабораторных занятий	**6**	
	Определение вариантов утечки информации по оптическим каналам для типовых контролируемых зон организации.	2	
	Изучение характеристик акустического канала утечки информации	2	
	Изучение характеристик радиоэлектронного канала утечки информации	2	
	В том числе самостоятельная работа обучающихся Основные понятия в области акустики	4	
Тема 1.5. Методы и средства технической разведки	**Содержание**	**4**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3.
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации.	2	

	Средства и возможности оптической разведки. Средства дистанционного съема информации.	2	ПК 3.4. ПК 3.5
	В том числе практических и лабораторных занятий	**4**	
	Изучение характеристик наземных средств дистанционного съема информации	2	
	Анализ современных средств перехвата сигналов	2	
Тема 1.6. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**8**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Акустоэлектрические преобразования.	2	
	Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.	2	
	Физические основы побочных электромагнитных излучений и наводок.	2	
	Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	2	
	В том числе практических и лабораторных занятий	**4**	
	Измерение параметров физических полей	2	
	Анализ современных средств перехвата сигналов	2	
	В том числе самостоятельная работа обучающихся Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Низкочастотные и высокочастотные излучения технических средств Физические основы побочных излучений и наводок	6	
Тема 1.7. Физические процессы при подавлении опасных сигналов	***Содержание***	**2**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		
	В том числе практических и лабораторных занятий	**4**	
	Изучение пассивных методов подавления опасных сигналов акустоэлектрических преобразователей	2	
	Изучение активных методов подавления опасных сигналов акустоэлектрических преобразователей	2	
	Содержание	**4**	ОК 09; ПК 3.1.

Тема 1.8. Системы защиты от утечки информации по акустическому каналу	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами.	2	ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	2	
	В том числе практических и лабораторных занятий	**4**	
	Анализ современных средств перехвата речевой информации	2	
	Защита от утечки по акустическому каналу	2	
	В том числе самостоятельная работа обучающихся Средства акустической разведки	4	
Тема 1.9. Системы защиты от утечки информации по проводному каналу	**Содержание**	**4**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов.	2	
	Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	2	
	В том числе практических и лабораторных занятий	**4**	
	Анализ способов технического закрытия от утечки речевой информации	2	
	Изучение сущности и параметров звукоизоляции	2	
	В том числе самостоятельная работа обучающихся Закладные устройства	2	
Тема 1.10. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**4**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи.	2	
	Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	2	
	В том числе практических и лабораторных занятий	**2**	
	Защита от утечки по виброакустическому каналу	2	
	Содержание	**6**	ОК 09; ПК 3.1.

Тема 1.11. Системы защиты от утечки информации по электромагнитному каналу	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры.	2	ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Системы защиты от утечки по электромагнитному каналу.	2	
	Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	2	
	В том числе практических и лабораторных занятий	**6**	
	Определение каналов утечки ПЭМИН	2	
	Защита от утечки по цепям электропитания и заземления	2	
	Изучение принципов работы и основных характеристик обнаружителей электромагнитного поля	2	
	В том числе самостоятельная работа обучающихся Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации с пассивных закладок.	4	
Тема 1.12. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**4**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке.	2	
	Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	2	
	В том числе практических и лабораторных занятий	**2**	
	Защита от утечки информации в средствах мобильной связи	2	
Тема 1.13. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**2**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	2	
	В том числе практических и лабораторных занятий	**4**	
	Изучение требований по защите системы электропитания объектов информатизации	2	
	Средства фильтрации опасных сигналов в цепях электропитания. Сетевые помехоподавляющие фильтры	2	
	Содержание	**2**	ОК 09; ПК 3.1.

Тема 1.14. Системы защиты от утечки информации по оптическому каналу	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.		ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	В том числе практических и лабораторных занятий	**4**	
	Изучение способов скрытого видеонаблюдения и съемки	2	
	Изучение способов защиты информации от утечки по оптическому каналу	2	
Тема 1.15. Применение технических средств защиты информации	**Содержание**	**8**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Технические средства для уничтожения информации и носителей информации, порядок применения.	2	
	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.	2	
	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.	2	
	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	2	
	В том числе практических и лабораторных занятий	**4**	
	Изучение характеристик технических средства для уничтожения информации и носителей информации	2	
	Изучение требований на комплексы и приборы, предназначенные для измерений характеристик побочных электромагнитных излучений и наводок	2	
Тема 1.16. Эксплуатация технических средств защиты информации	**Содержание**	**6**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.	2	
	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации.	2	
	Проведение аттестации объектов информатизации.	2	
	В том числе практических и лабораторных занятий	**8**	
	Установка и настройка технических средств защиты информации	2	
	Оценка функционирования средств защиты информации от несанкционированного доступа	2	

	Меры по защите информации на объекте информатизации.	2	
	Использование средств защиты информации. Реестр ФСТЭК России	2	
Обобщение разделов МДК		**4**	
Промежуточная аттестация по МДК.03.01	**экзамен**	**6**	
Раздел 2. Инженерно-технические средства физической защиты объектов информатизации		**236**	
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**138**	
Тема 2.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**10**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Характеристики потенциально опасных объектов.	2	
	Содержание и задачи физической защиты объектов информатизации.	2	
	Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации.	2	
	Модель нарушителя и возможные пути, и способы его проникновения на охраняемый объект.	2	
	Особенности задач охраны различных типов объектов.	2	
	В том числе практических и лабораторных занятий	**6**	
	Объект информатизации. Категорирование объектов информатизации	2	
	Модель нарушителя безопасности объекта информатизации	2	
	Типы охраны различных объектов и их обоснование при выборе помещения, как объекта защиты	2	
	В том числе самостоятельная работа обучающихся Виды злоумышленников. Разработка модели злоумышленника	4	
Тема 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**6**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты.	2	
	Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны.	2	
	Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	2	
	В том числе практических и лабораторных занятий	**6**	
	Типовые инженерные конструкции применяемые на объектах информатизации	2	

	Интегрированные системы обеспечения безопасности и их составляющие	2	
	Этапы построения системы защиты объекта	2	
Тема 2.3 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**8**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Информационные основы построения системы охранной сигнализации.	2	
	Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта.	2	
	Периметровые средства обнаружения: назначение, устройство, принцип действия.	2	
	Объектовые средства обнаружения: назначение, устройство, принцип действия.	2	
	В том числе практических и лабораторных занятий	**14**	
	Характеристики систем защиты территории и помещений, примеры технической реализации – инфракрасные системы, системы защиты ИК-датчиков, оптоволоконные системы	2	
	Характеристики систем защиты территории и помещений, примеры технической реализации – емкостные системы охраны периметров, вибрационные системы и вибрационно-сейсмические системы	2	
	Характеристики систем защиты территории и помещений, примеры технической реализации – радиолучевые системы, системы «активной» охраны периметров	2	
	Системы охранной, тревожной и пожарной сигнализации. Классификация извещателей охранных	2	
	Функциональные особенности некоторых применяемых на практике охранных и пожарных извещателей	2	
	Прибор приемно-контрольный (ППК) охранный (охранно-пожарный), классификация, параметры	2	
	Анализ рынка современных систем защиты территории и помещений	2	
	В том числе самостоятельная работа обучающихся Системы защиты территории и помещений. Системы активной охраны периметра. Системы оповещения	6	
Тема 2.4. Система контроля и управления доступом	**Содержание**	**8**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3.
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД.	2	

	Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД.	2	ПК 3.4. ПК 3.5
	Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.	2	
	Обнаружение металлических предметов и радиоактивных веществ.	2	
	В том числе практических и лабораторных занятий	**8**	
	Изучение принципов устройства, работы и применения аппаратных средств аутентификации и идентификации пользователя	2	
	Изучение принципов устройства, работы и применения средств контроля доступа	2	
	Биометрические системы идентификации, классификация. Этапы работы биометрических систем	2	
	Анализ рынка современных СКУД	2	
	В том числе самостоятельная работа обучающихся Атрибутные индентификаторы. Кодонаборные устройства	4	
Тема 2.5. Система телевизионного наблюдения	**Содержание**	**8**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Назначение системы телевизионного наблюдения.	2	
	Аналоговые и цифровые системы видеонаблюдения.	2	
	Состав системы телевизионного наблюдения. Видеокамеры. Объективы.	2	
	Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	2	
	В том числе практических и лабораторных занятий	**8**	
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	2	
	Изучение параметров видеокамер. Виды объективов.	2	
	Требования к качеству изображения. Технические решения, направленные на улучшение характеристик видеокамер	2	
	Варианты системы управления видеонаблюдением. Видеорегистраторы и их характеристики. Сетевое видеонаблюдение.	2	
	В том числе самостоятельная работа обучающихся Цели СОТ. Требования к качеству изображения. Видеоанализ и контроль объектов наблюдения.	4	

Тема 2.6. Система сбора, обработки, отображения и документирования информации	**Содержание**	**4**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации.	2	
	Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	2	
	В том числе практических и лабораторных занятий	**2**	
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	2	
Тема 2.7 Система воздействия	**Содержание**	**2**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	2	
	В том числе практических и лабораторных занятий	**2**	
	Обзор современных технических средств воздействия	2	
Тема 2.8 Применение инженерно-технических средств физической защиты	**Содержание**	**6**	
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом.	2	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места.	2	
	Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	2	
	В том числе практических и лабораторных занятий	**4**	
	Организация пропускного режима на КПП, система автоматического управления	2	
	Определение путей проникновения злоумышленника на объект информатизации	2	
	В том числе самостоятельная работа обучающихся Внутриобъектовый режим. Интегрированные охранные системы	4	
Тема 2.9. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**8**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.	2	
	Установка и настройка периметровых и объектовых технических средств обнаружения	2	

	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.	2	
	Организация ремонта технических средств физической защиты.	2	
	В том числе практических и лабораторных занятий	**2**	
	Изучение принципов диагностики, устранения отказов и восстановление работоспособности технических средств физической защиты	2	
Курсовая работа		**20**	
Обобщение разделов МДК		**4**	
Промежуточная аттестация по МДК.03.02	**экзамен**	**6**	
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. – Освоение методики выявления возможных угроз информационной безопасности объектов защиты. – Проектирование установки системы пожарно-охранной сигнализации по заданию. – Применение промышленных осциллографов, частотомеров и генераторов, и другого оборудования для защиты информации. – Рассмотрение системы контроля и управления доступом и её проектирование. – Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. – Рассмотрение датчиков периметра, их принципов работы. – Рассмотрение звукоизоляции помещений, обоснование зашумления и его проектирование. – Реализация защиты от утечки по цепям электропитания и заземления. – Разработка организационных и технических мероприятий по заданию. – Разработка основной документации по инженерно-технической защите информации.		**36**	
Производственная практика **Виды работ:**		***108***	

− Участие в монтаже, настройке, обслуживании и эксплуатации инженерной и технических средств защиты информации; − Участие в монтаже, настройке, обслуживании и эксплуатации средств охраны и безопасности; − Участие в монтаже, настройке, обслуживании и эксплуатации систем видеонаблюдения; − Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; − Участвовать в измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа; − Участвовать в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации; − Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами; − Освоение методики выявления возможных угрозы информационной безопасности объектов защиты; − Участие в организации отдельных работ по физической защите объектов информатизации − Разработка предложений по усовершенствованию технической защиты информации объекта информатизации.		
Экзамен по профессиональному модулю	***12***	
Всего	***492***	

2.4. Курсовая работа

Выполнение курсовой работы обязательно

Тематика курсовых работ

1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации.
2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации.
3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.
4. Моделирование объекта защиты и угроз безопасности информации для коммерческого предприятия
5. Разработка инженерно-технических мер по защите информации производственного объекта.
6. Разработка инженерно-технических мер по защите информации общественного учреждения
7. Разработка инженерно-технических мер по защите информации некоммерческой организации.

8. Разработка инженерно-технических мер по защите информации коммерческого предприятия
9. Разработка комплексной системы безопасности и мер по защите информации общественной организации
10. Комплексная система безопасности информации общественного здания
11. Расчет системы безопасности и контроля доступа коммерческой организации
12. Моделирование объекта защиты и угроз безопасности информации для некоммерческой организации
13. Расчет системы безопасности и контроля доступа производственного здания
14. Комплексная система безопасности информации коммерческой организации
15. Моделирование объекта защиты и угроз безопасности информации

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Мастерская «Кибербезопасности», оснащенная(ые) в соответствии с приложением 3 ОПОП-П.

Оснащенные базы практики (мастерские/зоны по видам работ), оснащенная(ые) в соответствии с приложением 3 ОПОП-П. . с п. 3.1.2. образовательной программы.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные 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.

5. 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. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/265178 (дата обращения: 20.07.2023). — Режим доступа: для авториз. пользователей.

6. 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. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/187645 (дата обращения: 20.07.2023). — Режим доступа: для авториз. пользователей.

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. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/336200 (дата обращения: 20.07.2023). — Режим доступа: для авториз. пользователей.

3.2.2. 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». [Электронный ресурс] – Режим доступа: http://window.edu.ru/resource/832/7832. Дата обращения 23.07.2022.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код ПК, ОК	Критерии оценки результата (показатели освоенности компетенций)	Формы контроля и методы оценки[1]
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрирует умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявляет умения и практический опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводит работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

[1] Примеры оформления формы контроля: контрольные работы, зачеты, квалификационные испытания, защита курсовых и дипломных проектов (работ), экзамены. Примеры оформления методов оценки: интерпретация результатов выполнения практических и лабораторных заданий, оценка решения ситуационных задач, оценка тестового контроля.

ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводит самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявляет знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	Понимает тексты на базовые профессиональные темы, участвует в диалогах на профессиональные темы обосновывает и объясняет свои действия, пишет простые связные сообщения на профессиональные темы	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

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

Рабочая программа профессионального модуля

«ПМ.04 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН»

2024 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.04 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН

1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «Оператор электронно-вычислительных и вычислительных машин».

Профессиональный модуль включен в обязательную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.2 Планируемые результаты освоения профессионального модуля

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

В результате освоения профессионального модуля обучающийся должен:

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
ПК 4.1	– 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	– Требования техники безопасности при работе с вычислительной техникой – Основные принципы устройства и работы компьютерных систем и периферийных устройств	– выполнять требования техники безопасности при работе с вычислительной техникой, – организовывать рабочее места оператора электронно-вычислительных и вычислительных машин, – подготовки оборудования компьютерной системы к работе
ПК 4.2	– Создавать и управлять содержимым документов с помощью текстовых процессоров – Создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц – Создавать и управлять содержимым презентаций с	– Классификацию и назначение компьютерных сетей – Виды носителей информации	– Инсталлировать, настраивать и обслуживать программное обеспечение компьютерной системы – Управлять файлами – Применять офисное программное обеспечение в соответствии с прикладной задачей

	помощью редакторов презентаций – Использовать мультимедиа проектор для демонстрации презентаций – Вводить, редактировать и удалять записи в базе данных – Эффективно пользоваться запросами базы данных – Создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики – Производить сканирование документов и их распознавание – Производить распечатку, копирование и тиражирование документов на принтере и других устройствах		
ПК 4.3	– 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	– Программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета	– Использовать ресурсы локальной вычислительной сети – Использовать ресурсы, технологии и сервисов Интернет
ПК 4.4	– Осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ – Осуществлять резервное копирование и восстановление данных	– Основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы	– Применять средства защиты информации в компьютерной системе

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Трудоемкость освоения модуля

Наименование составных частей модуля	**Объем в часах**	**В т.ч. в форме практической подготовки**
Учебные занятия	80	48
Курсовая работа (проект)		
Самостоятельная работа	14	
Практика, в т.ч.:		
учебная	144	144
производственная	96	96
Промежуточная аттестация, в том числе: *МДК 04.01 в форме диф. зачета* *УП 04* *ПП 04* *ПМ 04 экзамен*	12	
Всего	**346**	**288**

2.2. Структура профессионального модуля

Код ОК, ПК	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Обучение по МДК, в т.ч.:	Учебные занятия	Курсовая работа (проект)	Самостоятельная работа	Учебная практика	Производственная практика
1	2	3	4	5	6	7	8	9	10
ПК 4.1 - ПК 4.4	Раздел 1. Технология создания и обработки цифровой информации	94	48		80		14		
ПК 4.1- ПК 4.4	Учебная практика	144	144					144	
ПК 4.1- ПК 4.4	Производственная практика	96	96						96
ПК 4.1- ПК 4.4	Промежуточная аттестация	12							
	Всего:	**346**	**288**		**80**		**14**	**144**	**96**

2.3. Содержание профессионального модуля

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятия	Объем, ак. ч. / в том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
МДК 04.01 Технология создания и обработки цифровой информации			
Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения		***20***	
Тема 1.1. Работа с устройствами компьютерной системы	**Содержание**	**6**	
	Изучение охраны труда и техники безопасности Оператора ЭВМ. Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ	2	ПК 4.1 -ПК 4.4
	В том числе практических и лабораторных занятий		
	Подключение, настройка и подготовка к работе периферийного оборудования	2	
	Установка и замена расходных материалов для принтеров, ксерокса, сканера	2	
Тема 1.2. Работа с программным обеспечением компьютерной системы	**Содержание**	**6**	ПК 4.1 -ПК 4.4
	Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в Интернете	2	
	В том числе практических и лабораторных занятий		
	Изучение процесса установки операционной среды, настройка интерфейса ОС	2	
	Установка прикладных программ	2	
Тема 1.3. Диагностика неисправностей системы, ведение документации	**Содержание**	**8**	ПК 4.1 -ПК 4.4
	Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ	2	
	В том числе практических и лабораторных занятий		
	Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники	2	
	В том числе самостоятельная работа обучающихся	4	
Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах		***56***	
Тема 2.1.	**Содержание**	**12**	

Работа в текстовом процессоре	Текстовые процессоры. Требования по оформлению технической документации	2	ПК 4.1 -ПК 4.4
	В том числе практических и лабораторных занятий		
	Форматирование и редактирование шрифтов, абзацев и формул	2	
	Форматирование и редактирование списков	2	
	Работа с таблицами в текстовом процессоре	2	
	Работа с графическими объектами в текстовом процессоре	2	
	Форматирование документа в целом. Способы вывода документа на печать	2	
Тема 2.2. Работа в редакторе электронных таблиц	**Содержание**	**10**	
	Электронная таблица MS Excel. Ввод и редактирование данных. Создание и форматирование таблиц	2	ПК 4.1 -ПК 4.4
	Основы вычислений. Использование функций различных видов	2	
	В том числе практических и лабораторных занятий		
	Создание и форматирование таблицы в редакторе электронных таблиц	2	
	Вычисление с помощью формул в электронной таблице. Работа со встроенными функциями в электронной таблице.	2	
	Создание и работа с диаграммами и графиками. Обмен данными между текстовым процессором и электронной таблицей	2	
Тема 2.3. Работа в программе подготовки и просмотра презентаций	**Содержание**	**10**	
	Компьютерная презентация PowerPoint: основные и дополнительные возможности	2	ПК 4.1 -ПК 4.4
	Поэтапная разработка и настройка эффектов презентации	2	
	В том числе практических и лабораторных занятий		
	Основы работы со слайдом. Работа в презентации со шрифтом и текстом. Понятие темы слайда	2	
	Добавление в слайды рисунков, звуковых эффектов, таблиц и диаграмм	2	
	Настройка анимации объектов. Настройка показа и демонстрация результатов работы средствами мультимедиа	2	
Тема 2.4. Работа в системе управления базами данных	**Содержание**	**10**	
	Понятие базы данных и ее разновидности	2	ПК 4.1 -ПК 4.4
	Проектирование БД и разработка ее компонентов	2	
	В том числе практических и лабораторных занятий		

	Ввод данных в таблицы базы данных	2	
	Создание простых запросов и форм.	2	
	Создание и форматирование главной кнопочной формы. Создание отчетов.	2	
Тема 2.5. Работа в графических редакторах	**Содержание**	**14**	
	Инженерная графика. Системы автоматизированного проектирования.	2	ПК 4.1 -ПК 4.4
	Компьютерная графика. Основы работы в Adobe Photoshop.	2	
	В том числе практических и лабораторных занятий		
	Вставка и редактирование готового изображения с использованием программ растровой графики. Работа с цветом с использованием программ растрой графики.	2	
	Работа со слоями с использованием программ растрой графики. Работа со спецэффектами с использованием программ растровой графики.	2	
	В том числе самостоятельная работа обучающихся	6	
Раздел 3. Использование ресурсов технологий и сервисов Интернета		***6***	
Тема 3.1. Работа с ресурсами Интернета	**Содержание**	**6**	
	Создание и обмен письмами электронной почты. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера. Поиск, сортировка и анализ информации с помощью поисковых интернет-сайтов.	2	ПК 4.1 -ПК 4.4
	Пересылка и публикация файлов данных в Интернете.	2	
	В том числе самостоятельная работа обучающихся	2	
Раздел 4. Обеспечение защиты информации в компьютерной системе		***12***	
Тема 4.1. Защита информации при работе с офисными приложениями	**Содержание**	**12**	
	Использование штатных средств защиты информации в прикладных программах	2	ПК 4.1 -ПК 4.4
	Обеспечение безопасности в приложениях MS Office	2	
	В том числе практических и лабораторных занятий		
	Настройка парольной защиты на открытие и запись файла	2	
	Настройка защиты документа с помощью прав доступа	2	
	Защита информации в приложениях MS Office.	2	
	В том числе самостоятельная работа обучающихся	2	

Учебная практика **Виды работ** Подключение периферийных устройств к разъемам системного блока. Настройка и подготовка к работе принтера, сканера. Создание схем, таблиц и формул в программе Microsoft Word. Создание буклетов в программе Microsoft Publisher. Ведение расчетов и построение диаграмм в программе Microsoft Excel. Создание таблиц, форм, запросов и отчетов в программе Microsoft Access. Создание презентации в программе PowerPoint. Обработка графических объектов в Corel и PhotoShop. Настройка локальной вычислительной сети. Поиск информации в сети Интернет. Обработка графической информации Создание комплексного документа с использованием информации различных типов	**144**	
Производственная практика **Виды работ** Подготовка оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения. Создание и управление текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах. Использование ресурсов локальных вычислительных сетей и Интернета. Обеспечение защиты информации в компьютерной системе.	**96**	
Промежуточная аттестация	**12**	
Всего	**346**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Кабинет *«информационных технологий» (наименования кабинетов из указанных в п. 3.1.1. ОПОП-П),* оснащенный(е) в соответствии с приложением 3 ОПОП-П.

Мастерская и зоны по видам работы «веб-дизайн и разработка» *(перечисляются через запятую наименования мастерских из указанных в п. 3.1.2 ОПОП-П, необходимых для реализации модуля),* оснащенная(ые) в соответствии с приложением 3 ОПОП-П.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

Разработчики рабочей программы выбирают не менее одного издания из приведенного в ПОП-П перечня печатных и/или электронных образовательных изданий для использования в образовательном процессе.

3.2.2. Дополнительные источники:

1. Киселев С.В. Оператор ЭВМ: учеб. пособие для студ. учреждений сред. проф. образования /. – 7-е изд., испр. – М.: Издательский центр «Академия», 2014.

2. Коньков, К. А. Устройство и функционирование ОС Windows. Практикум к курсу Операционные системы. /Учебное пособие // К.А. Коньков. М.: Бином, Лаборатория знаний Интуит, 2013.

3. Струмпэ Н.В. Оператор ЭВМ. Практические работы: учеб. пособие для нач. проф. образования / – 6-е изд., стер. – М.: Издательский центр «Академия», 2013.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код ПК, ОК	Критерии оценки результата (показатели освоенности компетенций)	Формы контроля и 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
ПК 4.2 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	Проявление умения и практического опыта в работе с текстовыми документами, таблицами и презентациями, а также базами данных	
ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации	
ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе	Применение средств защиты информации в компьютерной системе	

Приложение 1.5
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа профессионального модуля

«ПМ.05 КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ»

2024 г

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ « ПМ.05 КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ»

1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: обеспечение комплексной системы защиты информации объекта информатизации.

Профессиональный модуль включен в вариативную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Планируемые результаты освоения профессионального модуля

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

В результате освоения профессионального модуля обучающийся должен:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК.09	– понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы – участвовать в диалогах на знакомые общие и профессиональные темы – строить простые высказывания о себе и о своей профессиональной деятельности – кратко обосновывать и объяснять свои действия (текущие и планируемые) – писать простые связные сообщения на знакомые или интересующие профессиональные темы	– правила построения простых и сложных предложений на профессиональные темы – основные общеупотребительные глаголы (бытовая и профессиональная лексика) – лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности – особенности произношения – правила чтения текстов профессиональной направленности	-
ПК 5.1.	– управлять защитой информации на объектах информатизации – проводить аудит защищенности информации на объекте информатизации – внедрять организационные меры по	– направления деятельности по организационной защите информации – требования по обеспечению информационной безопасности на объектах критической информационной инфраструктуры (КИИ), в отношении которых отсутствует необходимость	– внедрять программы и методики защиты на объектах – участвовать в оценке качества защиты объекта

	защите информации на объекте информатизации	присвоения им категорий значимости, в процессе их эксплуатации	
ПК 5.2.	– вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации – разработка организационно-распорядительных документов по защите информации на объектах защиты	– документы, определяющие регулирование отношений в области обеспечения безопасности КИИ – требования по обеспечению безопасности объектов информатизации, в том числе значимых объектов критической информационной инфраструктуры – виды носителей конфиденциальной безопасности информации	– готовить организационные документы, регламентирующие работу по защите информации – вести учет работ и объектов, подлежащих защите
ПК 5.3.	– находить уязвимости системы защиты информации – разрабатывать модели угроз модели угроз объекта информатизации	– модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ – требования к созданию систем безопасности объектов информатизации	– анализировать уязвимости системы защиты информации – определять причины возникновения угроз безопасности

1.3. Обоснование часов вариативной части ОПОП-П

№№ п/п	Дополнительные профессиональные компетенции	Дополнительные знания, умения, навыки	№, наимено-вание темы	Объем часов	Обоснование включения в рабочую программу
ПК 5.1	Участвовать в разработке и внедрении программ и методик организации защиты информации на объекте	**Навыки:** – Внедрять программы и методики защиты на объектах – Участвовать в оценке качества защиты объекта **Умения**: – Управлять защитой информации на объектах информатизации – Проводить аудит защищенности информации на объекте информатизации – Внедрять организационные меры по защите информации на объекте информатизации **Знания:** – Направления деятельности по организационной защите информации – Требования по обеспечению информационной безопасности на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации			
ПК 5.2	Осуществлять планирование и организацию выполнения мероприятий по защите информации	**Навыки:** – Готовить организационные документы, регламентирующие работу по защите информации – Вести учет работ и объектов, подлежащих защите **Умения:** – Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации			

		– Разработка организационно-распорядительных документов по защите информации на объектах защиты **Знания:** – Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ – Требования по обеспечению безопасности объектов информатизации, в том числе значимых объектов критической информационной инфраструктуры – Виды носителей конфиденциальной безопасности информации			
ПК 5.3	Выявлять и анализировать возможные угрозы информационной безопасности объектов	**Навыки:** – Анализировать уязвимости системы защиты информации – Определять причины возникновения угроз безопасности **Умения**: – Находить уязвимости системы защиты информации – Разрабатывать модели угроз модели угроз объекта информатизации **Знания:** – Модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ – Требования к созданию систем безопасности объектов информатизации			

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Трудоемкость освоения модуля

Наименование составных частей модуля	**Объем в часах**	**В т.ч. в форме практической подготовки**
Учебные занятия	164	96
Курсовая работа (проект)	-	-
Самостоятельная работа	16	
Практика, в т.ч.:	168	168
учебная	*48*	*48*
производственная	*120*	*120*
Промежуточная аттестация, в том числе: *МДК 05.01 в форме экзамена* *МДК 05.02. в форме экзамена* *МДК 05.03 в форме экзамена* *ПМ 05*	 6 6 6 12	
Всего	**378**	**264**

2.2. Структура профессионального модуля

Код ОК, ПК	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Обучение по МДК, в т.ч.:	Учебные занятия	Курсовая работа (проект)	Самостоятельная работа	Промежуточная аттестация	Учебная практика	Производственная практика
1	2	3	4	5	6	7	8		9	10
ОК 05; ПК 5.1. ПК 5.2. ПК 5.3.	**Раздел 1** Обеспечение безопасности ИТ-инфраструктуры объекта защиты	**70**	**32**	**70**	60	-	4	6		
ОК 05; ПК 5.1. ПК 5.2. ПК 5.3.	**Раздел 2** Организация и технология работы с конфиденциальной информацией	**64**	**32**	**64**	52	-	6	6		
ОК 05; ПК 5.1. ПК 5.2. ПК 5.3.	**Раздел 3** Комплексная системы защиты объекта	**64**	**32**	**64**	52	-	6	6		
	Учебная практика	**48**	**48**						**48**	
	Производственная практика	**120**	**120**							**120**
	Промежуточная аттестация	**12**						*12*		
	Всего:	**378**	**264**	**198**	***164***	**-**	***16***	***30***	**48**	**120**

2.3. Содержание профессионального модуля

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятия, курсовая работа (проект)	Объем, ак. ч. / в том числе в форме практической подготовки, ак. ч	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Обеспечение безопасности ИТ- инфраструктуры объекта защиты		**70/32**	
МДК.05.01 Обеспечение безопасности ИТ- инфраструктуры объекта защиты		**64/32**	
Тема 1.1. Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети объекта защиты	**Содержание**	**12**	ОК 05, ПК 5.1, ПК 5.2, ПК 5.3
	Принципы построения комплексных систем защиты информации	2	
	Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети	2	
	Основные механизмы защиты	2	
	В том числе практических и лабораторных занятий	**6**	
	Изучение руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации	2	
	Изучение порядка деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации	2	
	Изучение принципов построения комплексных систем защиты информации	2	
Тема 1.2. Основные механизмы защиты. Мониторинг и оперативное управление	**Содержание**	**16**	ОК 05, ПК 5.1, ПК 5.2, ПК 5.3
	Мониторинг и оперативное управление; полномочное управление доступом	2	
	Централизованная инвентаризация ресурсов локальной сети	2	
	Удаленный контроль работоспособности средств защиты информации на рабочих станциях	2	
	В том числе практических и лабораторных занятий	**10**	
	Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети.	2	
	Централизованная инвентаризация ресурсов локальной сети	2	
	Разграничение доступа к данным. Разграничение доступа к устройствам	2	
	Аудит событий информационной безопасности в КСЗИ	2	

	Замкнутая программная среда. Контроль целостности	2	
Тема 1.3. Управление системой безопасности ИТ- инфраструктуры объекта защиты	**Содержание**	**18**	ОК 05, ПК 5.1, ПК 5.2, ПК 5.3
	Управление серверами администрирования, управление группами администрирования	2	
	Управление клиентскими компьютерами, работа с отчетами, статистикой.	2	
	Централизованный учет и управление программно-аппаратными средствами защиты информации	2	
	В том числе практических и лабораторных занятий	**10**	
	Проведение инспекций и учет изменений конфигурации защищаемых рабочих станций	2	
	Работа со сведениями в журнале регистрации событий. Теневое копирование	2	
	Администрирование системы антивирусной защиты в локальной сети	2	
	Управление жизненным циклом средств аутентификации	2	
	Анализ доступных информационных источников с целью выявления известныхуязвимостей используемых в системе защиты информации программных и программно-аппаратных средств;	2	
	В том числе самостоятельная работа обучающихся Управление жизненным циклом и аудит средств аутентификации	**2**	
Тема 1.4. Нормативные требования по управлению средствами защиты информации	**Содержание**	**14**	ОК 05, ПК 5.1, ПК 5.2, ПК 5.3
	Анализ нормативных требований по управлению средствами защиты информации	2	
	Нормативные требования ФСТЭК при обеспечении мер безопасности персональных данных, в государственных информационных системах	2	
	Требования безопасности к автоматизированным системам управления технологическими процессами	2	
	В том числе практических и лабораторных занятий	**6**	
	Разработка политики безопасности информации автоматизированных систем	2	
	Разработка организационных мероприятий по обеспечению безопасности информации в автоматизированных системах	2	
	Оценка защищенности автоматизированных систем с помощью типовых программных средств	2	
	В том числе самостоятельная работа обучающихся Контроль работоспособности средств защиты информации на рабочих станциях	**2**	

Обобщение разделов МДК		**4**	
Промежуточная аттестация по МДК.05.01	**экзамен**	**6**	
Раздел 2. Организация и технология работы с конфиденциальной информацией		**64/32**	
МДК.05.02 Организация и технология работы с конфиденциальной информацией		**58/32**	
Тема 2.1. Организационные меры безопасности объектов защиты в том числе объектов КИИ	**Содержание**	**18**	ОК 05, ПК 5.1, ПК 5.2, ПК 5.3
	Характеристики потенциально опасных объектов. Понятие критической информационной инфраструктуры (КИИ)	2	
	Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ	2	
	Категорирование объектов информатизации Критерии значимости объектов КИИ РФ и их значения	2	
	В том числе практических и лабораторных занятий	**10**	
	Анализ документов, определяющих регулирование отношений в области обеспечения безопасности КИИ	2	
	Оценка безопасности объекта информатизации	2	
	Анализ Постановления от 8 февраля 2018 года №127. О порядке категорирования объектов критической информационной инфраструктуры	2	
	Анализ Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	2	
	Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России №31	2	
	В том числе самостоятельная работа обучающихся Виды злоумышленников и их возможностей	**2**	
Тема 2.2. Модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ	**Содержание**	**20**	ОК 05, ПК 5.1, ПК 5.2, ПК 5.3
	Классификация уязвимостей информационной системы, причины возникновения угроз безопасности. Нарушители ИБ объектов КИИ	2	
	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	2	
	Анализ угроз и разработка модели угроз	2	
	В том числе практических и лабораторных занятий	**12**	
	Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России №31	2	

	Определение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры	2	
	Анализ приказа № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»	2	
	Классификация уязвимостей информационной системы, причины возникновения угроз безопасности	2	
	Проектирование системы безопасности значимого объекта КИИ	4	
	В том числе самостоятельная работа обучающихся Состав системы безопасности значимых объектов.	**2**	
Тема 2.3 Организационно-распорядительные документы по обеспечению безопасности объектов в том числе объектов КИИ	**Содержание**	**16**	ОК 05, ПК 5.1, ПК 5.2, ПК 5.3
	Государственный контроль в области обеспечения безопасности значимых объектов КИИ	2	
	Правила выбора средств защиты информации для реализации организационных и технических мер.	2	
	В том числе практических и лабораторных занятий	**10**	
	Анализ организационно-распорядительных документов по безопасности значимых объектов	2	
	Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры	2	
	Изучение порядка и правил функционирования системы безопасности значимых объектов КИИ	2	
	Анализ приказа Федеральной службы по техническому и экспортному контролю № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»	2	
	Разработка рабочей и эксплуатационной документации.	2	
	В том числе самостоятельная работа обучающихся Определение порядка и правил обеспечения безопасности объектов	**2**	
Обобщение разделов МДК		**4**	
Промежуточная аттестация по МДК.05.02	**экзамен**	**6**	
Раздел 3. Обеспечение системы безопасности объекта защиты		**64/32**	
МДК.05.03 Обеспечение системы безопасности объекта защиты		**58/32**	

Тема 3.1. Структура комплексной системы безопасности	**Содержание**	**4**	ОК 05, ПК 5.1, ПК 5.2, ПК 5.3
	Основные подходы и требования к организации комплексной системы защиты информации.	2	
	Управление безопасностью	2	
	Оценка уязвимостей системы безопасности.		
	В том числе практических и лабораторных занятий	**8**	
	Составление организационной структуры организации и определение ее сферы деятельности	2	
	Выявление информационных активов организации	2	
	Выявление структурных единиц, работающих с конфиденциальной информацией	2	
	Анализ информационной системы объекта защиты	2	
	В том числе самостоятельная работа обучающихся Проведение аудита информационной безопасности виртуального предприятия	2	
Тема 3.2. Состав и структура системы безопасности	**Содержание**	**4**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Состав и структура системы безопасности. Направления защиты объекта информатизации.	2	
	Средства и способы защиты. Организации работы в чрезвычайной ситуации. Состав службы безопасности.	2	
	В том числе практических и лабораторных занятий	**2**	
	Разработка структуры системы безопасности организации	2	
Тема 3.3 Построение системы защиты информации	**Содержание**	**8**	ОК 09; ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5
	Планирование мероприятий по защите конфиденциальной информации	2	
	Формирование политики информационной безопасности на предприятии	2	
	Построение системы защиты информации объекта информатизации	2	
	Анализ рисков системы безопасности	2	
	В том числе практических и лабораторных занятий	**22**	
	Характеристика информации ограниченного доступа, циркулирующей на объекте защиты	2	
	Характеристика организационного обеспечения информационной безопасности	2	
	Характеристика системы контроля управления доступом объекта защиты	2	
	Характеристика инженерно-технического обеспечения системы защиты информации	2	

	Характеристика программно-аппаратного обеспечения системы защиты информации	2	
	Определение угроз информационной безопасности	2	
	Выделение недостатки существующей КСЗИ. Анализ рисков КСЗИ.	2	
	Усовершенствование организационного обеспечения и СКУД объекта защиты	2	
	Усовершенствование инженерно-технического обеспечение комплексной системы защиты информации	2	
	Усовершенствование программно-аппаратного обеспечения комплексной системы защиты информации	2	
	Анализ рисков разработанной КСЗИ	2	
	В том числе самостоятельная работа обучающихся Политика информационной безопасности в отечественных стандартах	2	
Обобщение разделов МДК		**4**	
Промежуточная аттестация по МДК.05.03	**экзамен**	**6**	
Учебная практика **Виды работ:** – Разграничение уровней политики информационной безопасности – Составление частной модели угроз для организации – Определение категории информационных ресурсов, подлежащих защите – Разработка мер обеспечения информационной безопасности» – Разработка основных принципов построения системы информационной безопасности – Выявление требований к аппаратным и программным средствам – Подбор антивирусного средства для конкретного объекта – Подготовка документа Политики информационной безопасности –		**48**	
Производственная практика **Виды работ:** – Анализ структуры организации и информационных процессов – Выявление опасностей и угроз объекта информатизации – Анализ структуры и типов защищаемой информации, по видам тайны и степеням конфиденциальности – Анализ существующей системы защиты объекта – Оценка степени защищенности объекта		***120***	

− Разработка нормативных документов необходимых для организации работы с персоналом, имеющим доступ к конфиденциальной информации − Разработка политики информационной безопасности − Разработка модели угроз информационной безопасности		
Экзамен по профессиональному модулю	***12***	
Всего	***378***	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Мастерская «Кибербезопасности», оснащенная(ые) в соответствии с приложением 3 ОПОП-П.

Оснащенные базы практики (мастерские/зоны по видам работ), оснащенная(ые) в соответствии с приложением 3 ОПОП-П. . с п. 3.1.2. образовательной программы.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. 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.

2. 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.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-fed eralnyj-zakon-ot-26-iyulya-2017-g-n-187-fz.

4. Постановление Правительства РФ № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_291398 .

5. Приказ Федеральной службы по техническому и экспортному контролю № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: https://rg.ru/2018/02/13/fstek-prikaz-227-site-dok.html .

6. Давыдова, Е. М. Организация защиты объектов критической информационной инфраструктуры: Учебно-методическое пособие [Электронный ресурс] / Е. М. Давыдова, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 20 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/10003.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код ПК, ОК	Критерии оценки результата (показатели освоенности компетенций)	Формы контроля и методы оценки
ПК 5.1 Участвовать в разработке и внедрении программ и методик организации защиты информации на объекте	Участвует в оценке качества защиты объекта Управляет защитой информации на объектах информатизации Проводит аудит защищенности информации на объекте информатизации Внедряет организационные меры по защите информации на объекте информатизации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 5.2 Осуществлять планирование и организацию выполнения мероприятий по защите информации	Готовит организационные документы, регламентирующие работу по защите информации Ведёт учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации Разрабатывает организационно-распорядительные документы по защите информации на объектах защиты	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 5.3 Выявлять и анализировать возможные угрозы информационной безопасности объектов	Проводит анализ уязвимостей системы защиты информации Определяет причины возникновения угроз безопасности Находит уязвимости системы защиты информации Разрабатываетмодели угроз модели угроз объекта информатизации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 09 Пользоваться профессиональной документацией на	Понимает тексты на базовые профессиональные темы, участвует в диалогах на профессиональные темы	Тестирование, экзамен квалификационный,

государственном и иностранном языках	обосновывает и объясняет свои действия, пишет простые связные сообщения на профессиональные темы	экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике