Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Нилова Екатерина Викторовна
Должность: Директор
Дата подписания: 25.11.2026 08:17:20
Уникальный программный ключ:
01b497467f3626bb4aa4f462dec308bcc7b24a93

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА»

УТВЕРЖДАЮ
Заместитель директора по учебной работе
_____ Л.А. Дьякова
« 26 » июня 2026 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования

по специальности 10.02.05 (код) Обеспечение информационной безопасности автоматизированных систем (Наименование специальности / профессии)

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
(Наименование дисциплины)

Кафедра разработчик Экономики и информационных дисциплин

Год набора 2023, 2024

2026 г.

Рабочая программа профессионального модуля
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
(наименование дисциплины согласно учебному плану)

Составлена *Кузнецовой Ириной Николаевной*
(Ф.И.О.)

Составлена
(Ф.И.О.)

Составлена
(Ф.И.О.)

Обсуждена и рекомендована к утверждению решением кафедры
экономики и информационных дисциплин

от 20.06.2026 протокол № 11
(дата протокола) *(номер протокола)*

Заведующий кафедрой *(подпись)* Г.И. Мирошниченко
(инициалы, фамилия)

Согласовано с выпускающей кафедрой
экономики и информационных дисциплин

Заведующий кафедрой *(подпись)* Г.И. Мирошниченко
(инициалы, фамилия)

Одобрена методическим советом

от 26.06.2026 протокол № 6
(дата протокола) *(номер протокола)*

Л.А. Дьякова

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ» …….. 6

2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ» ……... 12

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ» …….. 34

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ» ……..…….…… 35

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Цель и место профессионального модуля в структуре образовательной программы

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

Профессиональный модуль включен в обязательную часть образовательной программы.

1.2. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.

В результате освоения профессионального модуля обучающийся должен:

1.2.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.2.2. Перечень профессиональных компетенций

Код	Наименование общих компетенций
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с

	требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.2.3. В результате освоения профессионального модуля обучающийся должен:

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

1.2.4. В результате изучения профессионального модуля в соответствии с профессиональным стандартом «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. №536Н

(зарегистрирован Министерством юстиции Российской Федерации 18 октября 2022 года, регистрационный N 70596), обучающийся должен выполнять трудовые действия:

Код	Трудовые действия
A/01.5	– монтаж оборудования СССЭ; – первичная настройка и проверка функционирования СССЭ; – монтаж программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД; – установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НД; – первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД.
A/02.5	– текущий, в том числе автоматизированный, контроль функционирования СССЭ с установленными показателями; – текущий, в том числе автоматизированный, контроль функционирования с установленными показателями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи; – внесение изменений в настройки СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи без прерывания процесса их функционирования; – восстановление процесса функционирования после сбоев и отказов СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи; – восстановление значений показателей функционирования СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи.
A/03.5	– диагностика СССЭ штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами; – диагностика программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами; – выполнение предусмотренных регламентом операций по техническому обслуживанию средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи; – обновление в соответствии с регламентом эксплуатации программных компонентов СССЭ, программных, программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи; – устранение неисправностей СССЭ, а также программно-аппаратных

	(в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи своими силами, если это допускается технической документацией; – направление в ремонт и прием из ремонта сторонними организациями СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи; – ведение эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи.

В результате освоения профессионального модуля в соответствии с профессиональным стандартом «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. №525н (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2022 г., регистрационный №70543), обучающийся должен выполнять трудовые действия

Код	Трудовые действия
A/01.5	– 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.
A/02.5	– ведение документов учета, обработки, хранения и передачи информации ограниченного доступа; – информирование персонала об угрозах безопасности информации; – информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации; – ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем; – ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем; – ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем; – подготовка сведений об отсутствии необходимости присвоения категорий значимости объекту критической информационной инфраструктуры, на котором используется автоматизированная система, и направление в письменном виде этих сведений в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной им форме.
A/03.5	– включение в организационно-распорядительные документы по защите информации процедур уничтожения (стирания) информации на

	машинных носителях, а также контроля уничтожения (стирания) информации; – уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания); – физическое уничтожение машинных носителей информации, обрабатываемой автоматизированной системой; – Архивирование информации, обрабатываемой автоматизированной системой.

1.2.5. Перечень личностных результатов реализации программы воспитания

Код	**Личностные результаты реализации программы воспитания** *(дескрипторы)*
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности	
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм
ЛР 15	Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
Личностные результаты реализации программы воспитания, определенные субъектом Российской Федерации	
ЛР 16	Самостоятельный и ответственный в принятии решений во всех сферах своей деятельности, готовый к исполнению разнообразных социальных ролей, востребованных бизнесом, обществом и государством
ЛР 17	Открытый к текущим и перспективным изменениям в мире труда и профессий
ЛР 19	Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики.
ЛР 20	Экономически активный, предприимчивый, готовый к самозанятости.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

максимальной учебной нагрузки обучающегося – 714 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 672 часов;
практические работы- 208 часов:
самостоятельной работы обучающегося – 16 часов;
учебной практики – 144 часов;
практики по профилю специальности- 108 часов;
консультаций - 14 часов;
промежуточной аттестации - 12 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ»

2.1. Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)						Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося			Учебная, часов	Производственная (по профилю специальности)
			Всего, часов	в т. ч. лабораторные работы и практические занятия, часов	в т. ч., курсовая работа (проект), часов	Всего, часов	в т. ч., курсовая работа (проект), часов	в т. ч. консультации		
1	2	3	4	5	6	7	8	9	10	11
ПК 1.1 - ПК 1.3	МДК 01.01. Операционные системы	80	76	36	-	4	-	2	-	-
ПК 1.1 - ПК 1.3	МДК 01.02. Базы данных	80	76	40	-	4	-	2	-	-
ПК 1.2 – ПК 1.4	МДК 01.03. Сети и системы передачи информации	42	38	20	-	4	-	2	-	-
ПК 1.1 - ПК 1.4	МДК 01.04. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	134	124	50	-	10	-	4		
ПК 1.1 - ПК 1.4	МДК 01.05. Эксплуатация компьютерных сетей	114	106	62	-	8	-	4		
ПК 1.1 – ПК 1.4	Учебная практика по ПМ. 01	144	-	-	-	-	-		144	-
ПК 1.1 - ПК 1.4	Производственная практика по ПМ.01	108	-	-	-	-	-		-	108
	Всего:	558	420	208		30		14	144	108

2.2. Содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа студента, курсовая работа (проект)		Объем часов
1	2		3
Раздел 1 Операционные системы			80
МДК.01.01 Операционные системы			
Тема 1.1. Основы теории операционных систем	Содержание учебного материала		6
	1.	Определение операционной системы. Основные понятия. История развития операционных систем.	
	2.	Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением.	
	3.	Системные вызовы. Исследования в области операционных систем.	
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	Содержание учебного материала		8
	1.	Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС.	
	2.	Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.	
	3.	Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.	
	Практические занятия		8
	1.	Виртуальные машины. Создание, модификация, работа.	
	2.	Установка ОС.	
	3.	Создание и изучение структуры разделов жесткого диска.	
	4.	Операции с файлами.	
Тема 1.3. Модульная структура операционных систем,	Содержание учебного материала		2
	1.	Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.	

пространство пользователя	Практические занятия		2
	1.	Работа в консольном и графическом режимах.	
Тема 1.4. Управление памятью	Содержание учебного материала		2
	1.	Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти.	
	Практические занятия		2
	1.	Мониторинг за использованием памяти.	
Тема 1.5. Управление процессами, многопроцессорные системы	Содержание учебного материала		4
	1.	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие.	
	2.	Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок.	
	Практические занятия		4
	1.	Управление процессами.	
	2.	Наблюдение за использованием ресурсов системы.	
Тема 1.6. Виртуализация и облачные технологии	Содержание учебного материала		6
	1.	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации.	
	2.	Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования.	
	3.	Облачные технологии. Исследования в области виртуализации и облаков.	
	Практические занятия		2
	1.	Изучение примеров виртуальных машин (VMware, VBox).	
Тема 1.7. Принципы построения защиты информации в операционных системах	Содержание учебного материала		6
	1.	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия.	
	2.	Порядок обеспечения безопасности информации при эксплуатации операционных систем. Штатные средства ОС для защиты информации.	
	3.	Аутентификация, авторизация, аудит.	
	Практические занятия		6
	1.	Управление учетными записями пользователей и доступом к ресурсам.	

	2.	Аудит событий системы.	
	3.	Изучение штатных средств защиты информации в операционных системах.	
Тема 1.8. Операционные системы UNIX, Linux, MacOS и Android	Содержание учебного материала		6
	1.	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX.	
	2.	Операционные системы семейства Mac OS: особенности, преимущества и недостатки.	
	3.	Архитектура Android. Приложения Android.	
	Практические занятия		4
	1.	Создание дистрибъютива Linux. Установка.	
	2.	Работа в ОС Linux.	
Тема 1.9. Операционная система Windows	Содержание учебного материала		2
	1.	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	
	Практические занятия		4
	1.	Установка и первичная настройка Windows.	
Тема 1.10. Серверные операционные системы	Содержание учебного материала		2
	1.	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	
	Практические занятия		4
	1.	Работа с сетевой файловой системой.	
	2.	Работа с серверной ОС, например, AltLinux.	
Самостоятельная работа при изучении МДК 01.01. Операционные системы			2
Примерная тематика внеаудиторной самостоятельной работы Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите. 1. Создание виртуальной машины. 2. Установка операционной системы. 3. Анализ журнала аудита ОС на рабочем месте. 4. Изучение аналитических обзоров в области построения систем безопасности операционных систем.			
Консультации			2

Раздел 2 Базы данных			80
МДК 01.02. Базы данных			
Тема 2.1. Основные понятия теории баз данных. Модели данных	Содержание учебного материала		6
	1.	Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования.	
	2.	Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных.	
	3.	Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	
Тема 2.2. Основы реляционной алгебры	Содержание учебного материала		2
	1.	Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	
	Практические занятия		2
	1.	Операции над отношениями.	
Тема 2.3. Базовые понятия и классификация систем управления базами данных	Содержание учебного материала		2
	1.	Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору).	
Тема 2.4. Целостность данных как ключевое понятие баз данных	Содержание учебного материала		2
	1.	Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	
Тема 2.5. Информационные модели реляционных баз данных	Содержание учебного материала		2
	1.	Типы информационных моделей. Логические модели данных. Физические модели данных.	
	Практические занятия		2
	1.	Проектирование инфологической модели данных.	
Тема 2.6. Нормализация таблиц реляционной базы	Содержание учебного материала		2
	1.	Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам. Дальнейшая нормализация таблиц. Четвертая и пятая	

данных. Проектирование связей между таблицами		нормальные формы. Применение процесса нормализации.	
	Практические занятия		2
	1.	Проектирование структуры базы данных.	
Тема 2.7. Средства автоматизации проектирования	Содержание учебного материала		2
	1.	CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	
	Практические занятия		2
	1.	Проектирование базы данных с использованием CASE-средств.	
Тема 2.8. Создание базы данных. Манипулирование данными	Содержание учебного материала		2
	1.	Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.	
	Практические занятия		2
	1.	Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	
Тема 2.9. Индексы. Связи между таблицами. Объединение таблиц	Содержание учебного материала		2
	1.	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	
	Практические занятия		4
	1.	Создание взаимосвязей.	
	2.	Сортировка, поиск и фильтрация данных. Способы объединения таблиц.	
Тема 2.10. Структурированный язык запросов SQL	Содержание учебного материала		2
	1.	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	
	Практические занятия		2
	1.	Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL.	
Тема 2.11. Операторы и	Содержание учебного материала		2

функции языка SQL	1.	Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	
	Практические занятия		4
	1.	Создание и использование запросов. Группировка и агрегирование данных.	
	2.	Коррелированные вложенные запросы. Создание в запросах вычисляемых полей. Использование условий.	
Тема 2.12. Архитектуры распределенных баз данных	Содержание учебного материала		2
	1.	Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных.	
	Практические занятия		2
	1.	Управление доступом к объектам базы данных.	
Тема 2.13. Серверная часть распределенной базы данных	Содержание учебного материала		2
	1.	Планирование и развёртывание СУБД для работы с клиентскими приложениями.	
	Практические занятия		2
	1.	Установка СУБД. Настройка компонентов СУБД.	
Тема 2.14. Клиентская часть распределенной базы данных	Содержание учебного материала		2
	1.	Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация. Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа. Оптимизация производительности работы СУБД.	
	Практические занятия		6
	1.	Создание форм и отчетов.	
	2.	Создание меню. Генерация, запуск.	
	3.	Профилирование запросов клиентских приложений.	
Тема 2.15. Обеспечение целостности, достоверности и непротиворечивости	Содержание учебного материала		2
	1.	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.	

данных	Практические занятия		2
	1.	Разработка хранимых процедур и триггеров.	
Тема 2.16. Перехват исключительных ситуаций и обработка ошибок	Содержание учебного материала		2
	1.	Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	
Тема 2.17. Механизмы защиты информации в системах управления базами данных	Содержание учебного материала		2
	1.	Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД.	
	Практические занятия		4
	1.	Средства защиты информации в базах данных.	
	2.	Управление правами доступа к базам данных.	
Тема 2.18. Копирование и перенос данных. Восстановление данных	Содержание учебного материала		2
	1.	Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных.	
	Практические занятия		4
	1.	Аудит данных с помощью средств СУБД и триггеров.	
	2.	Резервное копирование и восстановление баз данных.	
Самостоятельная работа при изучении МДК 01.02. Базы данных			2
Примерная тематика внеаудиторной самостоятельной работы: Выполнение индивидуального задания по теме «Проектирование инфологической модели базы данных». Выполнение индивидуального задания по теме «Нормализация отношений». Подготовка рефератов на тему «Развитие СУБД» (конкретной СУБД). Выполнение индивидуального задания по теме «Создание базы данных. Создание таблиц. Организация межтабличных связей» Выполнение индивидуального задания по теме «Организация запросов». Выполнение индивидуального задания по теме «Создание пользовательского приложения средствами СУБД».			

Разбор синтаксиса хранимых процедур и триггеров. Подготовка рефератов по теме «Организация и использование механизмов защиты базы данных»			
Консультации			2
Раздел 3 Сети и системы передачи информации			42
МДК 01.03. Сети и системы передачи информации			
Тема 3.1. Основные понятия и определения	Содержание учебного материала		4
	1.	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов.	
	2.	Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	
Тема 3.2. Принципы передачи информации в сетях и системах связи	Содержание учебного материала		4
	1.	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход.	
	2	Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	
Тема 3.3. Типовые каналы передачи и их характеристики	Содержание учебного материала		4
	1.	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи.	
	2.	Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ.	
	Практические занятия		2
	1.	Расчет пропускной способности канала связи.	
Тема 3.4. Архитектура и принципы работы современных сетей передачи данных	Содержание учебного материала		6
	1.	Структура и характеристики сетей. Способы коммутации и передачи данных.	
	2.	Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи.	
	3.	Протоколы и интерфейсы управления каналами и сетью передачи данных.	
	Практические занятия		12
	1.	Конфигурирование сетевого интерфейса рабочей станции.	
	2.	Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP.	
	3.	Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне.	
	4.	Диагностика и разрешение проблем сетевого уровня.	
	5.	Диагностика и разрешение проблем протоколов транспортного уровня.	
	6.	Диагностика и разрешение проблем протоколов прикладного уровня.	

Тема 3.5. Беспроводные системы передачи данных	Содержание учебного материала		2
	1.	Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX.	
	Практические занятия		4
	1.	Настройка Wi-Fi маршрутизатора.	
Тема 3.6. Сотовые и спутниковые системы	Содержание учебного материала		2
	1.	Сети и системы сотовой связи.	
	Практические занятия		2
	1.	Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.	
Самостоятельная работа при изучении МДК 01.03. Сети и системы передачи информации			2
Примерная тематика внеаудиторной самостоятельной работы Структурирование и обобщение информации Настройка Wi-Fi маршрутизатора Изучение сетевых утилит Конфигурирование сетевого интерфейса Маршрутизация и управление потоками в сетях связи			
Консультации			2
Раздел 4 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении			134
МДК 01.04. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении			
Тема 4.1. Основы информационных систем как объекта защиты	Содержание учебного материала		6
	1.	Понятие автоматизированной (информационной) системы. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС.	
	2.	Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.	
	3.	Основные особенности современных проектов АИС. Электронный документооборот.	
	Практические занятия		2
	1.	Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании).	
Тема 4.2. Жизненный	Содержание учебного материала		8

цикл автоматизированных систем	1.	Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные.	
	2.	Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.	
	3.	Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.	
	4.	Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.	
	Практические занятия		2
	1.	Разработка технического задания на проектирование автоматизированной системы.	
Тема 4.3. Угрозы безопасности информации в автоматизированных системах	Содержание учебного материала		6
	1.	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации.	
	2.	Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации.	
	3.	Понятие уязвимости угрозы. Классификация уязвимостей.	
	Практические занятия		6
	1.	Категорирование информационных ресурсов.	
	2.	Анализ угроз безопасности информации.	
	3.	Построение модели угроз.	
Тема 4.4. Основные меры защиты информации в автоматизированных системах	Содержание учебного материала		4
	1.	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	
	2.	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним.	
Тема 4.5. Содержание и порядок эксплуатации АС в защищенном исполнении	Содержание учебного материала		18
	1.	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа	
	2.	Ограничение программной среды. Защита машинных носителей информации. Регистрация событий безопасности.	
	3.	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения.	

	4.	Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	
	5.	Обнаружение (предотвращение) вторжений.	
	6.	Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации.	
	7.	Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.	
	8.	Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных.	
	9.	Резервное копирование и восстановление данных. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	
	Практические занятия		10
	1.	Управление доступом субъектов доступа к объектам доступа.	
	2.	Защита машинных носителей информации.	
	3.	Регистрация событий безопасности.	
	4.	Обнаружение (предотвращение) вторжений.	
	5.	Резервное копирование и восстановление данных.	
Тема 4.6. Защита информации в распределенных автоматизированных системах	Содержание учебного материала		4
	1.	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем.	
	2.	Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	
Тема 4.7. Особенности разработки информационных систем персональных данных	Содержание учебного материала		4
	1.	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.	
	2.	Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	
	Практические занятия		2
	1.	Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	
Тема 4.8. Особенности эксплуатации автоматизированных	Содержание учебного материала		6
	1.	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	
	2.	Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных	

систем в защищенном исполнении		систем.	
	3.	Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении.	
	Практические занятия		4
	1.	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	
	2.	Выполнение работ по защите информации при модернизации автоматизированной системы в защищенном исполнении.	
Тема 4.9. Администрирование автоматизированных систем	Содержание учебного материала		4
	1.	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями.	
	2.	Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	
Тема 4.10. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	Содержание учебного материала		2
	1.	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	
	Практические занятия		2
	1.	Порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.	
Тема 4.11. Защита от несанкционированного доступа к информации	Содержание учебного материала		6
	1.	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.	
	2.	Классификация автоматизированных систем. Требования по защите информации от НСД для АС.	
	3.	Требования защищенности СВТ от НСД к информации. Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ.	
	Практические занятия		4
	1.	Защита информации от НСД для АС.	
	2.	Средства защиты, обеспечивающие безопасное взаимодействие сетей ЭВМ	

Тема 4.12. Средства защиты информации от несанкционированного доступа	Содержание учебного материала		10
	1.	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты.	
	2.	Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.	
	3.	Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий.	
	4.	Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.	
	5.	Обеспечение целостности информационной системы и информации. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.	
	Практические занятия		14
	1.	Установка и настройка СЗИ от НСД.	
	2.	Защита входа в систему (идентификация и аутентификация пользователей).	
	3.	Разграничение доступа к устройствам. Управление доступом.	
	4.	Использование принтеров для печати конфиденциальных документов. Контроль печати.	
	5.	Настройка системы для задач аудита.	
	6.	Настройка контроля целостности и замкнутой программной среды.	
	7.	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.	
Тема 4.13. Эксплуатация средств защиты информации в компьютерных сетях	Содержание учебного материала		4
	1.	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.	
	2.	Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении. Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.	
	Практические занятия		2
	1.	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем.	
Тема 4.14.	Содержание учебного материала		2

Документация на защищаемую автоматизированную систему	1.	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	
	Практические занятия		2
	1.	Оформление основных эксплуатационных документов на автоматизированную систему.	
Самостоятельная работа при изучении МДК 01.04. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении			6
Примерная тематика внеаудиторной самостоятельной работы Разработка концепции защиты автоматизированной (информационной) системы Анализ банка данных угроз безопасности информации Анализ журнала аудита ОС на рабочем месте Построение сводной матрицы угроз автоматизированной (информационной) системы Анализ политик безопасности информационного объекта Изучение аналитических обзоров в области построения систем безопасности Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации			
Консультации			4
Раздел 5. Эксплуатация компьютерных сетей			114
МДК.01.05. Эксплуатация компьютерных сетей			
Тема 5.1. Модели сетевого взаимодействия	Содержание учебного материала		4
	1.	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.	
	2.	Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	
	Практические занятия		2
	1.	Изучение элементов кабельной системы.	
Тема 5.2. Физический уровень модели OSI	Содержание учебного материала		4
	1.	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи. Методы совместного использования среды передачи канала связи.	
	2.	Мультиплексирование и методы множественного доступа. Оптоволоконные линии связи. Стандарты кабелей. Электрическая проводка. Беспроводная среда передачи.	
	Практические занятия		2

	1.	Создание сетевого кабеля на основе неэкранированной витой пары (UTP). Сварка оптического волокна.	
Тема 5.3. Топология компьютерных сетей	Содержание учебного материала		2
	1.	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.	
	Практические занятия		4
	1.	Разработка топологи сети небольшого предприятия.	
	2.	Построение одноранговой сети.	
Тема 5.4. Технологии Ethernet	Содержание учебного материала		2
	1.	Обзор технологий построения локальных сетей. Технология Ethernet. Физический уровень. Технология Ethernet. Канальный уровень.	
	Практические занятия		2
	1.	Изучение адресации канального уровня. MAC-адреса.	
Тема 5.5. Технологии коммутации	Содержание учебного материала		4
	1.	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI. Конструктивное исполнение коммутаторов.	
	2.	Физическое стекирование коммутаторов. Программное обеспечение коммутаторов. Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети. Технология PoweroverEthernet.	
	Практические занятия		2
	1.	Создание коммутируемой сети.	
Тема 5.6. Сетевой протокол IPv4	Содержание учебного материала		2
	1.	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов. Маршрутизация пакетов IPv4. Протоколы динамической маршрутизации.	
	Практические занятия		2
	1.	Изучение IP-адресации.	
Тема 5.7. Скоростные и беспроводные сети	Содержание учебного материала		2
	1.	Сеть FDDI. Сеть 100VG-AnyLAN. Сверхвысокоскоростные сети. Беспроводные сети.	
	Практические занятия		2
	1.	Настройка беспроводного сетевого оборудования.	
Тема 5.8. Основы коммутации	Содержание учебного материала		2
	1.	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах. Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов.	
	Практические занятия		2

	1.	Работа с основными командами коммутатора.	
Тема 5.9. Начальная настройка коммутатора	Содержание учебного материала		2
	1.	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора. Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.	
	Практические занятия		4
	1.	Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов.	
	2.	Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы.	
Тема 5.10. Виртуальные локальные сети (VLAN)	Содержание учебного материала		4
	1.	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN.	
	2.	Протокол GVRP. Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation.	
	Практические занятия		6
	1.	Настройка VLAN на основе стандарта IEEE 802.1Q. Настройка протокола GVRP.	
	2.	Настройка сегментации трафика без использования VLAN. Настройка функции Q-in-Q (Double VLAN).	
	3.	Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.	
Тема 5.11. Функции повышения надежности и производительности	Содержание учебного материала		2
	1.	Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP. Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol. Дополнительные функции защиты от петель. Агрегирование каналов связи.	
	Практические занятия		4
	1.	Настройка протоколов связующего дерева STP, RSTP, MSTP.	
	2.	Настройка функции защиты от образования петель LoopBackDetection. Агрегирование каналов.	
Тема 5.12. Адресация сетевого уровня и маршрутизация	Содержание учебного материала		2
	1.	Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса. Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса. Планирование подсетей IPv6. Протокол NDP. Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.	
	Практические занятия		6

	1.	Основные конфигурации маршрутизатора. Расширенные конфигурации маршрутизатора. Работа с протоколом CDP.	
	2.	Работа с протоколом TELNET. Работа с протоколом TFTP. Работа с протоколом RIP. Работа с протоколом OSPF.	
	3.	Конфигурирование функции маршрутизатора NAT/PAT. Конфигурирование PPP и CHAP.	
Тема 5.13. Качество обслуживания (QoS)	Содержание учебного материала		4
	1.	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	
	2.	Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.	
	Практические занятия		2
	1.	Настройка QoS. Приоритизация трафика. Управление полосой пропускания.	
Тема 5.14. Функции обеспечения безопасности и ограничения доступа к сети	Содержание учебного материала		2
	1.	Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора. Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.	
	Практические занятия		2
	1.	Списки управления доступом (AccessControlList). Контроль над подключением узлов к портам коммутатора. Функция PortSecurity. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding.	
Тема 5.15. Многоадресная рассылка	Содержание учебного материала		2
	1.	Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки. Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping).Функция IGMP FastLeave.	
	Практические занятия		4
	1.	Отслеживание трафика многоадресной рассылки.	
	2.	Отслеживание трафика Multicast.	
Тема 5.16. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	Содержание учебного материала		2
	1.	Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры. Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.	
	Практические занятия		4
	1.	Управление конфигурациями сетевой инфраструктуры.	

	2.	Управление инцидентами безопасности.	
Тема 5.17. Межсетевые экраны	Содержание учебного материала		4
	1.	Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.	
	2.	Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.	
	Практические занятия		
	1.	Основы администрирования межсетевого экрана.	8
	2.	Соединение двух локальных сетей межсетевыми экранами.	
	3.	Создание политики без проверки состояния. Создание политик для традиционного (или исходящего) NAT.	
	4.	Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing.	
Тема 5.18. Системы обнаружения и предотвращения проникновений	Содержание учебного материала		2
	1.	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства. Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.	
	Практические занятия		4
	1.	Обнаружение и предотвращение вторжений.	
Тема 5.19. Приоритизация трафика и создание альтернативных маршрутов	Содержание учебного материала		2
	1.	Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.	
	Практические занятия		2
	1.	Создание альтернативных маршрутов с использованием статической маршрутизации.	
Самостоятельная работа при изучении МДК 01.05. Эксплуатация компьютерных сетей			4
Примерная тематика внеаудиторной самостоятельной работы Физическое кодирование с использованием манчестерского кода Логическое кодирование с использованием скремблирования Подключение клиента к беспроводной сети в инфраструктурном режиме Оценка беспроводной линии связи Проектирования беспроводной сети Сбор информации о клиентских устройствах Планирование производительности и зоны действия беспроводной сети			

Консультации	4
Учебная практика по модулю Виды работ 1. Установка программного обеспечения в соответствии с технической документацией. 2. Настройка параметров работы программного обеспечения, включая системы управления базами данных. 3. Настройка компонентов подсистем защиты информации операционных систем. 4. Управление учетными записями пользователей. 5. Работа в операционных системах с соблюдением действующих требований по защите информации. 6. Установка обновления программного обеспечения. 7. Контроль целостность подсистем защиты информации операционных систем. 8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных 9. Использование программных средств для архивирования информации. 10. Проведение аудита защищенности автоматизированной системы. 11. Установка, настройка и эксплуатация сетевых операционных систем. 12. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 13. Организация работ с удаленными хранилищами данных и базами данных. 14. Организация защищенной передачи данных в компьютерных сетях. 15. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. 16. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. 17. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	144
Производственная практика по модулю Виды работ 1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения 3. Настройка программного обеспечения с соблюдением требований по защите информации 4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам 5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением 6. Настройка встроенных средств защиты информации программного обеспечения 7. Проверка функционирования встроенных средств защиты информации программного обеспечения 8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения	108

9. Обслуживание средств защиты информации в компьютерных системах и сетях 10. Обслуживание систем защиты информации в автоматизированных системах 11. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем 12. Проверка работоспособности системы защиты информации автоматизированной системы 13. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации 14. Контроль стабильности характеристик системы защиты информации автоматизированной системы 15. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем 16. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРИМЕРНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Реализация программы предполагает наличие учебного кабинета «Общепрофессиональных дисциплин и профессиональных модулей», лаборатории «Информационных технологий, программирования и баз данных».

Оборудование учебного кабинета и рабочих мест кабинета:

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

Оборудование лаборатории и рабочих мест лаборатории:

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

4.2 Информационное обеспечение обучения

1. Внуков, А. А. Защита информации в банковских системах: учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2024. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537248

2. Внуков, А. А. Основы информационной безопасности: защита информации: учебник для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458

3. 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, 2026. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588246

4. Компьютерные сети: учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва: Издательство Юрайт, 2026. — 515 с. — (Профессиональное образование). — ISBN 978-5-534-21453-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590199

5. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567521

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе выполнения заданий практической направленности.

Результаты (освоенные общие, профессиональные компетенции, а также личностные результаты)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Контрольные работы, зачеты, квалификационные испытания, защита курсовых проектов, экзамены. Интерпретация результатов выполнения практических заданий, оценка решения ситуационных задач, оценка тестового контроля.
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных	

	(информационных) систем в защищенном исполнении	
ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Наблюдение; мониторинг, оценка содержания портфолио студента; результаты участия в конкурсах, конференциях (призовые места; свидетельства об участии; звания лауреатов)
ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	Мониторинг и рейтинг выполнения работ на учебной практике; практических работ по решению профессиональных задач по разработке и модификации информационных систем
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	составляет и корректирует индивидуальный план профессионального и личностного развития; определяет перспективные направления развития профессиональных умений и планирует мероприятия по их освоению (курсы, стажировки, конкурсы профмастерства); применяет знания правовой грамотности при анализе типовых ситуаций профессиональной деятельности (оформление документов, трудовые отношения, договоры); применяет знания финансовой грамотности при решении практических задач (планирование бюджета, оценка финансовой целесообразности решений); демонстрирует понимание основ предпринимательской деятельности в профессиональной сфере и	Наблюдение и оценка на практических занятиях; при выполнении работ по учебной практике.

	возможностей самозанятости; осуществляет самоанализ и самооценку результатов собственной деятельности	
ОК 4. Эффективно взаимодействовать и работать в коллективе и команде	взаимодействует с участниками команды, распределяя и принимая роли и обязанности; предлагает и принимает решения в интересах команды, согласуя их с общей целью; выполняет порученную часть командной работы в установленные сроки и с требуемым качеством; проявляет толерантность к различным точкам зрения, учитывает мнения участников команды; конструктивно разрешает конфликтные ситуации в коллективе; осуществляет самооценку и взаимооценку результатов совместной деятельности	Тестирование; подготовка рефератов, докладов, эссе.
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	излагает информацию устно на государственном языке Российской Федерации грамотно, логично и доступно (защита отчёта, доклад, участие в обсуждении); готовит письменные документы профессионального назначения (отчёты, акты, журналы, пояснительные записки) с соблюдением норм делового стиля; адаптирует форму и содержание коммуникации к собеседнику и ситуации; корректно воспринимает и интерпретирует полученную информацию, задаёт уточняющие вопросы; соблюдает нормы делового	Подготовка и защита проектов с использованием ИКТ; наблюдение за навыками работы в глобальных и локальных информационных сетях.

	и речевого этикета в профессиональной среде; представляет результаты выполненной работы аудитории	
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	демонстрирует осознанное поведение на основе традиционных российских духовно-нравственных ценностей (человекоцентричность, милосердие, справедливость, коллективизм, историческая память, служение Отечеству, крепкая семья, созидательный труд, приоритет духовного над материальным); проявляет уважительное отношение к людям разных национальностей и конфессий, не допускает дискриминационного поведения; соблюдает стандарты антикоррупционного поведения: не допускает использования служебного положения в личных целях, следует принципам честности и добросовестности; проявляет уважение к государственным символам Российской Федерации, историческому и культурному наследию страны; участвует в социально значимых мероприятиях и волонтёрской деятельности	Защита проектов командой; наблюдение и оценка роли обучающихся в группе.
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно	соблюдает правила экологической безопасности при работе с оборудованием и утилизации отходов (отработавшие носители информации,	Оценка качества и сроков выполнения командных работ; тестирование; анкетирование; наблюдение, мониторинг и интерпретация результатов наблюдений за

действовать в чрезвычайных ситуациях	аккумуляторы, оргтехника); применяет принципы ресурсосбережения: рациональное использование электроэнергии, расходных материалов, повторное использование компонентов; применяет принципы бережливого производства: устранение потерь, наведение порядка на рабочем месте, стандартизация операций; демонстрирует знание причин и последствий изменения климата и роли профессиональной деятельности в снижении негативного воздействия на окружающую среду; действует в соответствии с планом при возникновении чрезвычайных ситуаций: эвакуация, первая помощь, средства индивидуальной защиты, вызов экстренных служб	деятельностью обучающегося в процессе освоения образовательной программы
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	выполняет комплексы упражнений для профилактики утомления при работе за компьютером (зрительная гимнастика, упражнения для мышц спины, шеи, кистей рук); организует рабочее место и режим труда с соблюдением требований эргономики и здоровьесбережения; применяет средства физической культуры для поддержания необходимого уровня физической подготовленности (самостоятельные занятия, производственная гимнастика); соблюдает режим дня,	Результаты защиты проектных работ и презентации творческих работ (открытые защиты творческих и проектных работ); сдача квалификационных экзаменов и зачетов по программам ДПО; контроль графика выполнения индивидуальной самостоятельной работы обучающегося.

	труда и отдыха в период прохождения практики; проводит самооценку уровня физической подготовленности и корректирует двигательную активность	
ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках	эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	Оценка практических занятий, презентаций, докладов и рефератов; учебно-практические конференции; конкурсы профессионального мастерства.
Итоговая аттестация по профессиональному модулю –*квалификационный экзамен*		

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ» ……..……. 6
2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ» ……... 12
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ» ……... 32
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ» ..…… 34

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 образовательной программы.

1.2. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.

В результате освоения профессионального модуля обучающийся должен: освоить основной вид деятельности «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и соответствующие ему общие компетенции, профессиональные компетенции и личностные результаты:

1.2.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;
ОК 9.	Пользоваться профессиональной документацией на государственном и

	иностранном языках.

1.2.2. Перечень профессиональных компетенций

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

1.2.3. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	В: – установке и настройке программных средств защиты информации; – тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; – учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.
уметь	- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; - использовать типовые программные криптографические средства, в том числе электронную подпись; - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
знать	- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

	- основные понятия криптографии и типовых криптографических методов и средств защиты информации.

1.2.4. В результате освоения профессионального модуля в соответствии с профессиональным стандартом «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449), обучающийся должен выполнять трудовые действия:

Код	Трудовые действия
A/02.5	– текущий, в том числе автоматизированный контроль функционирования СССЭ с установленными показателями; – текущий, в том числе автоматизированный контроль функционирования с установленными показателями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; – внесение изменений в настройки СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД без прерывания процесса их функционирования; – восстановление процесса функционирования после сбоев и отказов СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД; – восстановление значений показателей функционирования СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД;
A/03.5	– диагностика программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами; – обновление в соответствии с регламентом эксплуатации программных компонентов СССЭ, программных, программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД; – устранение неисправностей СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД своими силами, если это допускается технической документацией; – направление в ремонт и прием из ремонта сторонними организациями СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; – ведение эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД.

В результате освоения профессионального модуля в соответствии с профессиональным стандартом «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 01 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)

Код	Трудовые действия
A/01.5	– ввод в эксплуатацию программно-аппаратных средств защиты информации в операционных системах; – установка программно-аппаратных средств защиты информации; – настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам; – установка средств антивирусной защиты в соответствии с действующими требованиями; – инструктаж пользователей по порядку безопасной работы в операционных системах; – оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах; – восстановление работоспособности программно-аппаратных средств защиты информации в операционных системах согласно технической документации; – проверка корректности работы программно-аппаратных средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
A/02.5	– ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях; – установка программно-аппаратных средств защиты информации в компьютерных сетях; – установка средств межсетевого экранирования в соответствии с действующими требованиями по защите информации; – настройка программно-аппаратных средств защиты информации в компьютерных сетях по заданным шаблонам; – устранение неисправностей программно-аппаратных средств защиты информации в компьютерных сетях согласно технической документации; – инструктаж пользователей по порядку безопасной работы в компьютерных сетях; – оформление эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях;
A/03.5	– установка программного обеспечения; – настройка программного обеспечения с соблюдением требований по защите информации; – настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам; – инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением; – настройка встроенных средств защиты информации программного обеспечения по заданным шаблонам; – проверка функционирования встроенных средств защиты информации программного обеспечения; – своевременное обнаружение признаков наличия вредоносного программного обеспечения.

В результате освоения профессионального модуля в соответствии с профессиональным стандартом «Специалист по защите информации в

автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. №522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016г., регистрационный №43857), обучающийся должен выполнять трудовые действия:

Код	Трудовые действия
А/01.5	– контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации – контроль стабильности характеристик системы защиты информации автоматизированной системы;
А/02.5	– ведение документов учета, обработки, хранения и передачи информации, составляющей тайну – информирование персонала об угрозах безопасности информации – информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации – ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем – ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем – ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем;
А/03.5	– уничтожение информации, обрабатываемой автоматизированной системой – уничтожение машинных носителей информации, обрабатываемой автоматизированной системой – архивирование информации, обрабатываемой автоматизированной системой.

1.2.5. Перечень личностных результатов реализации программы воспитания

Код	Личностные результаты реализации программы воспитания *(дескрипторы)*
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности	
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм
ЛР 15	Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и

	общественной деятельности
Личностные результаты реализации программы воспитания, определенные субъектом Российской Федерации	
ЛР 16	Самостоятельный и ответственный в принятии решений во всех сферах своей деятельности, готовый к исполнению разнообразных социальных ролей, востребованных бизнесом, обществом и государством
ЛР 17	Открытый к текущим и перспективным изменениям в мире труда и профессий
ЛР 19	Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики.
ЛР 20	Экономически активный, предприимчивый, готовый к самозанятости.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

максимальной учебной нагрузки обучающегося – 724 часа, включая:
обязательной аудиторной учебной нагрузки обучающегося – 658 часов;
практические работы- 162 часа:
самостоятельной работы обучающегося – 30 часов;
учебной практики – 108 часов;
практики по профилю специальности- 108 часов;
консультаций - 24 часа;
промежуточной аттестации - 12 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)						Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося			Учебная, часов	Производственная (по профилю специальности)
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов	в т. ч. консультации		
1	2	3	4	5	6	7	8	9	10	11
ПК 2.1 - ПК 2.6	МДК 02.01. Программно-аппаратные средства защиты информации в автоматизированных системах	202	180	48	30	22	-	10	-	-
ПК 2.1 - ПК 2.6	МДК 02.02. Криптографические средства защиты информации в автоматизированных системах	162	144	56	-	18	-	8	-	-
ПК 2.1 - ПК 2.6	МДК 02.03. Комплексное обеспечение информационной безопасности в автоматизированных системах	132	118	58	-	14	-	6	-	-
ПК 2.1 - ПК 2.6	Учебная практика по ПМ. 02	108	-	-	-	-	-		108	-
ПК 2.1 - ПК 2.6	Производственная практика по ПМ. 02	108	-	-	-	-	-		-	108
	Всего:	712	362	162	30	54		24	108	108

2.2. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа студента, курсовая работа (проект)		Объем часов
1	2		3
Раздел 1. Программные и программно-аппаратные средства защиты информации			202
МДК.02.01 Программно-аппаратные средства защиты информации в автоматизированных системах			
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание учебного материала		6
	1.	Предмет и задачи программно-аппаратной защиты информации.	
	2.	Основные понятия программно-аппаратной защиты информации.	
	3.	Классификация методов и средств программно-аппаратной защиты информации.	
Тема 1.2. Стандарты безопасности	Содержание учебного материала		4
	1.	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.	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
	Практические занятия		6
	1.	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.	
	2.	Работа с содержанием нормативных правовых актов.	
	3.	Обзор стандартов. Работа с содержанием стандартов.	
Тема 1.3. Защищенная автоматизированная	Содержание учебного материала		4
	1.	Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности	

система		автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.	
	2.	Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС. Дискреционные модели. Мандатные модели.	
	Практические занятия		6
	1.	Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа.	
	2.	Регистрация событий (аудит). Контроль целостности данных. Уничтожение остаточной информации.	
	3.	Управление политикой безопасности. Шаблоны безопасности. Криптографическая защита. Обзор программ шифрования данных.	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	Содержание учебного материала		6
	1.	Источники дестабилизирующего воздействия на объекты защиты.	
	2.	Способы воздействия на информацию.	
	3.	Причины и условия дестабилизирующего воздействия на информацию.	
	Практические занятия		2
	1.	Распределение каналов в соответствии с источниками воздействия на информацию.	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Содержание учебного материала		8
	1.	Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД.	
	2.	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.	
	3.	Доступ к данным со стороны процесса.	
	4.	Особенности защиты данных от изменения. Шифрование.	
	Практические занятия		2
	1.	Организация доступа к файлам. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД.	
Тема1.6. Основы защиты автономных	Содержание учебного материала		8
	1.	Работа автономной АС в защищенном режиме.	

автоматизированных систем	2.	Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды.	
	3.	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка).	
	4.	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	
Тема 1.7. Защита программ от изучения	Содержание учебного материала		6
	1.	Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение.	
	2.	Задачи защиты от изучения и способы их решения. Защита от отладки.	
	3.	Защита от дизассемблирования. Защита от трассировки по прерываниям.	
Тема 1.8. Вредоносное программное обеспечение	Содержание учебного материала		14
	1.	Вредоносное программное обеспечение как особый вид разрушающих воздействий.	
	2.	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.	
	3.	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	
	4.	Бот-неты. Принцип функционирования. Методы обнаружения.	
	5.	Классификация антивирусных средств. Сигнатурный и эвристический анализ.	
	6.	Защита от вирусов в «ручном режиме».	
	7.	Основные концепции построения систем антивирусной защиты на предприятии.	
	Практические занятия		2
	1.	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО.	
Тема 1.9. Защита программ и данных от несанкционированного копирования	Содержание учебного материала		4
	1.	Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.	
	2.	Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении на примере MS Office.	

	Практические занятия		4
	1.	Защита информации от несанкционированного копирования с использованием специализированных программных средств.	
	2.	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint).	
Тема 1.10. Защита информации на машинных носителях	Содержание учебного материала		6
	1.	Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование.	
	2.	Средства восстановления остаточной информации. Создание посекторных образов НЖМД. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов.	
	3.	Безвозвратное удаление данных. Принципы и алгоритмы.	
	Практические занятия		8
	1.	Применение средства восстановления остаточной информации на примере Foremost или аналога.	
	2.	Применение специализированного программного средства для восстановления удаленных файлов.	
	3.	Применение программ для безвозвратного удаления данных.	
	4.	Применение программ для шифрования данных на съемных носителях.	
Тема 1.11. Аппаратные средства идентификации и аутентификации пользователей	Содержание учебного материала		4
	1.	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ.	
	2.	Устройства Touch Memory.	
Тема 1.12. Системы обнаружения атак и вторжений	Содержание учебного материала		4
	1.	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ. Использование сетевых снифферов в качестве СОВ. Аппаратный компонент СОВ. Программный компонент СОВ.	
	2.	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
	Практические занятия		2
	1.	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений.	

Тема 1.13. Основы построения защищенных сетей	Содержание учебного материала		4
	1.	Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации.	
	2.	Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	
Тема 1.14. Средства организации VPN	Содержание учебного материала		4
	1.	Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN.	
	2.	Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.	
	Практические занятия		4
	1.	Развертывание VPN.	
Тема 1.15. Обеспечение безопасности межсетевого взаимодействия	Содержание учебного материала		8
	1.	Методы защиты информации при работе в сетях общего доступа.	
	2.	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall.	
	3.	Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня.	
	4.	Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов.	
	Практические занятия		2
	1.	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr. Изучение различных способов закрытия «опасных» портов.	
Тема 1.16. Защита информации в базах данных	Содержание учебного материала		6
	1.	Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом.	
	2.	Средства контроля целостности информации в базах данных. Средства аудита и контроля	

		безопасности. Критерии защищенности баз данных.	
	3.	Применение криптографических средств защиты информации в базах данных.	
	Практические занятия		2
	1.	Изучение механизмов защиты СУБД MS Access. Изучение штатных средств защиты СУБД MSSQL Server.	
Тема 1.17. Мониторинг систем защиты	Содержание учебного материала		4
	1.	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25. Классификация отслеживаемых событий. Особенности построения систем мониторинга.	
	2.	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
	Практические занятия		2
	1.	Проведение аудита ЛВС сетевым сканером.	
Тема 1.18. Изучение мер защиты информации в информационных системах	Содержание учебного материала		2
	1.	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	
	Практические занятия		2
	1.	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	
Тема 1.19. Изучение современных программно-аппаратных комплексов	Практические занятия		4
	1.	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов.	
	2.	Изучение типовых решений для построения VPN на примере VipNet или других аналогов.	
Самостоятельная работа при изучении МДК 02.01. Программно-аппаратные средства защиты информации в автоматизированных системах			12
Примерная тематика внеаудиторной самостоятельной работы			

Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим занятиям с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите. 1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты 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 7. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов	
Консультации	10
Обязательная аудиторная учебная нагрузка по курсовому проекту	30
Примерная тематика курсовых проектов 1. Разработка системы защиты информации информационной системы коммерческого предприятия. 2. Анализ внешних угроз сети торгового предприятия. 3. Создание структуры программно-аппаратных средств защиты информации коммерческого предприятия. 4. Защита жесткого диска персонального компьютера от проникновения с помощью программных средств. 5. Защита базы данных предприятия криптографическими методами. 6. Настройка прав пользователей к базам данных коммерческого предприятия. 7. Разработка политики учетных записей коммерческого предприятия. 8. Разработка групповой политики безопасности OS Windows для сотрудников государственного учреждения. 9. Обеспечение сохранности конфиденциальной информации с использованием встроенных в ОС средств защиты. 10. Внедрение программно-аппаратного комплекса в систему защиты организации. 11. Создание защищенной системы предприятия с использованием межсетевых экранов и маршрутизаторов. 12. Обеспечение защиты от вредоносного программного обеспечения и сетевых атак OS Windows с помощью программных средств. 13. Обеспечение целостности данных коммерческого предприятия с помощью резервного копирования. 14. Настройка и конфигурирование средств собственной защиты Windows. 15. Разработка системы защиты информации информационной системы учебного учреждения. 16. Внедрение в сеть организации межсетевого экрана и аппаратного брандмауэра. 17. Построение защищенного VPN между филиалами организации.	

18. Построение схемы защиты организации с помощью программно-аппаратных средств. 19. Передача электронной отчетности предприятия с использованием криптографических систем. 20. Построение защиты информации предприятия с помощью шифрования жесткого диска. 21. Шифрование данных предприятия при передаче по сети Интернет. 22. Настройка защиты сервера организации с помощью электронного ключа. 23. Проектирование комплекса программно-аппаратных средств защиты предприятия. 24. Разработка защиты локальной сети с использованием управляемых маршрутизаторов и защиты портов. 25. Использование в системе защиты Монитора безопасности субъекта и Монитора безопасности объекта. 26. Защита информации на серверах с помощью отказоустойчивых томов. 27. Защита сервера базы данных с помощью программно-аппаратных средств. 28. Разработка входа в Информационную систему с использование биометрических параметров. 29. Построение замкнутой информационной системы. 30. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных. 31. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов. 32. Реализация защищенного входа в ОС Windows на базе расширений UEFI. 33. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей. 34. Анализ методов и средств анализа защищенности беспроводных сетей. 35. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 36. Средства обеспечения информационной безопасности банков данных. 37. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации. 38. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота. 39. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа. 40. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации 41. Инструментальные средства анализа рисков информационной безопасности. 42. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности)	
Раздел 2. Криптографические средства защиты информации		162
МДК 02.02. Криптографические средства защиты информации		
Введение	Содержание учебного материала	2

	1.	Предмет и задачи криптографии. История криптографии. Основные термины.	
Тема 2.1. Математические основы криптографии	Содержание учебного материала		24
	1.	Элементы теории множеств. Группы, кольца, поля.	
	2.	Делимость чисел. Признаки делимости. Простые и составные числа.	
	3.	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	
	4.	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	
	5.	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	
	6.	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	
	7.	Китайская теорема об остатках.	
	8.	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	
	9.	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	10.	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	11.	Арифметические операции над большими числами.	
	12.	Эллиптические кривые и их приложения в криптографии.	
	Практические занятия		6
	1.	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений.	
	2.	Проверка чисел на простоту.	
	3.	Решение задач с элементами теории чисел.	
Тема 2.2. Методы криптографической защиты информации	Содержание учебного материала		8
	1.	Классификация основных методов криптографической защиты. Методы симметричного шифрования.	
	2.	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.	
	3.	Методы перестановки. Табличная перестановка, маршрутная перестановка.	
	4.	Гаммирование. Гаммирование с конечной и бесконечной гаммами.	
	Практические занятия		6
	1.	Применение классических шифров замены.	
	2.	Применение классических шифров перестановки.	

	3.	Применение метода гаммирования.	
Тема 2.3. Криптоанализ	Содержание учебного материала		6
	1..	Основные методы криптоанализа. Криптографические атаки.	
	2.	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса.	
	3.	Перспективные направления криптоанализа, квантовый криптоанализ.	
	Практические занятия		8
	1.	Криптоанализ шифра простой замены методом анализа частотности символов.	
	2.	Криптоанализ классических шифров методом полного перебора ключей.	
	3.	Криптоанализ шифра Вижинера.	
Тема 2.4. Поточные шифры и генераторы псевдослучайных чисел	Содержание учебного материала		6
	1.	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	
	2.	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	Практические занятия		2
	1.	Применение методов генерации псевдослучайных чисел	
Тема 2.5. Кодирование информации. Компьютеризация шифрования.	Содержание учебного материала		8
	1.	Кодирование информации. Символьное кодирование. Смысловое кодирование.	
	2.	Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.	
	3.	Компьютеризация шифрования. Аппаратное и программное шифрование. Стандартизация программно-аппаратных криптографических систем и средств.	
	4.	Изучение современных программных и аппаратных криптографических средств.	
	Практические занятия		6
	1.	Кодирование информации.	
	2.	Программная реализация классических шифров.	
	3.	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	
Тема 2.6. Симметричные системы шифрования	Содержание учебного материала		4
	1.	Общие сведения. Структурная схема симметричных криптографических систем.	
	2.	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.	
	Практические занятия		2
	1.	Изучение программной реализации современных симметричных шифров.	
Тема 2.7. Асимметричные системы шифрования	Содержание учебного материала		6
	1.	Криптосистемы с открытым ключом. Необратимость систем.	
	2.	Структурная схема шифрования с открытым ключом.	
	3.	Элементы теории чисел в криптографии с открытым ключом.	
	Практические занятия		4
	1.	Применение различных асимметричных алгоритмов.	
	2.	Изучение программной реализации асимметричного алгоритма RSA.	
Тема 2.8. Аутентификация данных. Электронная подпись	Содержание учебного материала		4
	1.	Аутентификация данных. Общие понятия. ЭП. MAC.	
	2.	Однонаправленные хеш-функции. Алгоритмы цифровой подписи.	
	Практические занятия		8
	1.	Применение различных функций хеширования, анализ особенностей хешей.	
	2.	Применение криптографических атак на хеш-функции.	
	3.	Изучение программно-аппаратных средств, реализующих основные функции ЭП.	
Тема 2.9. Алгоритмы обмена ключей и протоколы аутентификации	Содержание учебного материала		4
	1.	Алгоритмы распределения ключей с применением симметричных и асимметричных схем.	
	2.	Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация.	
	Практические занятия		6
	1.	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	
	2.	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
Тема 2.10. Криптозащита информации в сетях передачи данных	Содержание учебного материала		6
	1.	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей.	
	2.	Криптомаршрутизатор. Пакетный фильтр.	
	3.	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
Тема 2.11. Защита	Содержание учебного материала		4

информации в электронных платежных системах	1.	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер.	
	2.	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	Практические занятия		4
	1.	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей.	
Тема 2.12. Компьютерная стеганография	Содержание учебного материала		6
	1.	Скрытая передача информации в компьютерных системах.	
	2.	Проблема аутентификации мультимедийной информации. Защита авторских прав.	
	3.	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ.	
	Практические занятия		4
	1.	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ.	
	2.	Реализация простейших стеганографических алгоритмов.	
Самостоятельная работа при изучении МДК 02.02. Криптографические средства защиты информации			10
Примерная тематика внеаудиторной самостоятельной работы: 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Методы механизации шифрования 5. Цифровое представление различных форм информации 6. Анализ современных симметричных криптоалгоритмов 7. Анализ современных асимметричных криптоалгоритмов 8. Программная реализация современных криптоалгоритмов 9. Сравнительный анализ функций хеширования 10. Аутентификация сообщений 11. Законодательство в области криптографической защиты информации 12. Перспективные направления криптографии			
Консультации			8
Раздел 3. Комплексное обеспечение информационной безопасности			132
МДК 02.03. Комплексное обеспечение информационной безопасности в автоматизированных системах			
Тема 3.1. Введение в	Содержание учебного материала		4

дисциплину. Сущность комплексной защиты информации и принципы ее организации	1.	Понятие, сущность и назначение комплексной защиты информации, ее задач для обеспечения деятельности предприятия.	
	2.	Принципы организации комплексной системы защиты информации.	
	Практические занятия		2
	1.	Комплексная система защиты информации на предприятии и принципы ее организации.	
Тема 3.2. Методологические и концептуальные основы комплексной системы защиты информации	Содержание учебного материала		6
	1.	Методология защиты информации и ее основные задачи. Уровень обеспечения безопасности информации.	
	2.	Достаточность защиты информации. Варианты построения комплексной защиты информации.	
	3.	Основные факторы, влияющие на организацию комплексной системы защиты информации. Характер и степень влияния различных факторов на организацию системы защиты информации.	
	Практические занятия		4
	1.	Оценка факторов, влияющих на организацию комплексной системы защиты информации.	
Тема 3.3. Определение и нормативное закрепление информации ограниченного доступа	Содержание учебного материала		4
	1.	Классификация информации по видам тайны и степеням конфиденциальности. Этапы работы по выявлению состава защищаемой информации.	
	2.	Нормативное закрепление состава защищаемой информации. Порядок организации нормативного закрепления информации ограниченного доступа.	
	Практические занятия		6
	1.	Определение основных бизнес-процессов на предприятии.	
	2.	Этапы работы по выявлению состава защищаемой информации на предприятии.	
Тема 3.4. Определение состава объектов защиты	Содержание учебного материала		6
	1.	Понятие объекта защиты. Последовательность определения объекта защиты.	
	2.	Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации.	
	3.	Методика выявления состава носителей защищаемой информации. Основные и вспомогательные технические средства и системы. Особенности помещений как объектов защиты.	
	Практические занятия		6
	1.	Определение состава объектов защиты информации на предприятии.	
	2.	Формирование перечня сведений конфиденциального характера на предприятии.	

Тема 3.5. Источники, способы результаты дестабилизирующего воздействия на информацию	Содержание учебного материала		6
	1.	Определение источников дестабилизирующего воздействия на информацию. Модель формирования множества дестабилизирующих факторов.	
	2.	Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации.	
	3.	Классификация угроз безопасности информации как объекта информатизации. Анализ и оценка угроз информационной безопасности объекта.	
	Практические занятия		6
	1.	Классификация угроз безопасности информации для объекта информатизации на предприятии.	
	2.	Анализ и оценка угроз информационной безопасности объекта информатизации.	
Тема 3.6. Выявление каналов утечки и методов несанкционированного воздействия на информацию	Содержание учебного материала		6
	1.	Сущность утечки информации и несанкционированного воздействия на информацию. Структурная модель канала утечки информации.	
	2.	Технические каналы утечки информации и их классификация. Модель технических каналов утечки и информации на типовом объекте информатизации.	
	3.	Каналы утечки из-за несанкционированного воздействия на информацию и системы, использующие информационно-коммуникационные технологии. Инсайдерские каналы утечки информации и «социальный реинжиниринг». Методы «социального реинжиниринга».	
	Практические занятия		4
	1.	Выявление каналов утечки информации на предприятии.	
Тема 3.7. Моделирование процессов защиты информации	Содержание учебного материала		6
	1.	Понятие модели и объекта моделирования. Основные виды моделей и их характеристика. Задачи и этапы моделирования в процессе построения комплексной системы защиты информации.	
	2.	Понятие архитектуры системы защиты информации. Кибернетическая, функциональная, информационная и организационная модели комплексной системы защиты информации.	
	3.	Формальные модели безопасности. Теории и методы моделирования процессов защиты информации.	
	Практические занятия		6
	1.	Задачи и этапы моделирования в процессе построения комплексной системы защиты информации.	
	2.	Разработка модели технических каналов утечки информации на типовом объекте информатизации предприятия.	
	3.	Моделирование процессов защиты информации.	
Тема 3.8.	Содержание учебного материала		6

Технологическое и организационное построение комплексной защиты информации	1.	Общее содержание работ по организации комплексной системы защиты информации. Характеристика технологического и организационного направлений создания комплексной системы защиты информации.	
	2.	Содержание стадий построения комплексной системы защиты информации. Предпроектное обследование. Назначение и структура технического задания, технико-экономического обоснования.	
	3.	Технический проект, рабочий проект. Апробация системы защиты информации и ввод ее в эксплуатацию.	
	Практические занятия		10
	1.	Разработка технико-экономического обоснования комплексной системы защиты информации.	
	2.	Технологическое построение комплексной системы защиты информации.	
	3.	Организационное построение комплексной системы защиты информации.	
Тема 3.9. Кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации	Содержание учебного материала		6
	1.	Кадровое обеспечение функционирования комплексной системы защиты информации. Защита человеческих ресурсов. Распределение функций по защите информации.	
	2.	Материально-техническое обеспечение защиты информации. Нормативно-методическое обеспечение комплексной защиты информации на предприятии.	
	3.	Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.	
	Практические занятия		4
	1.	Разработка нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.	
Тема 3.10. Планирование и контроль комплексной системы защиты информации	Содержание учебного материала		6
	1.	Понятие, принципы и методы планирования комплексной системы защиты информации. Стадии планирования. Факторы, влияющие на выбор принципов и способов планирования.	
	2.	Структура и общее содержание планов предприятия и функционирования комплексной системы защиты информации. Организация выполнения планов.	
	3.	Сущность, цель, задачи и содержание контроля комплексной системы защиты информации. Основные контрольные мероприятия по защите информации.	
	Практические занятия		2
	1.	Организация планирования и контроля комплексной системы защиты информации на предприятии.	
Тема 3.11. Оценка	Содержание учебного материала		4

эффективности комплексной системы защиты информации	1.	Понятие эффективности и эффективности защиты информации. Требования по защите информации. Показатель и норма эффективности защиты информации. Подходы к оценке эффективности систем защиты информации и их особенности.	
	2.	Состав методов и моделей оценки эффективности систем защиты информации. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативной документации.	
	Практические занятия		8
	1.	Применение методов и моделей оценки эффективности систем защиты информации.	
	2.	Состав и содержание нормативно-правовых актов по аттестации объектов информатизации.	
	3.	Организация и проведение процедур аттестации объектов информатизации по требованиям безопасности информации.	
Самостоятельная работа при изучении МДК 01.03. Комплексное обеспечение информационной безопасности в автоматизированных системах			8
Примерная тематика внеаудиторной самостоятельной работы 1. Характер и степень влияния различных факторов на организацию систем защиты информации. 2. Порядок организации нормативного закрепления информации ограниченного доступа. 3. Базовые модели угроз безопасности различных видов информации ограниченного доступа. 4. Методы «социального инжиниринга». 5. Апробация системы защиты и ввод ее в эксплуатацию. 6. Основные контрольные мероприятия по защите информации. 7. Основы проведения поисковых мероприятий по выявлению закладочных устройств. 8. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации.			
Консультации			6
Учебная практика по модулю Виды работ 1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах. 2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности. 3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности. 4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации.			108

5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации. 6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. 7. Устранение замечаний по результатам проверки. 8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. 9. Применение математических методов для оценки качества и выбора наилучшего программного средства. 10. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.	
Производственная практика по модулю Виды работ 1. Анализ принципов построения систем информационной защиты производственных подразделений. 2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; 3. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении 4. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации 5. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	108

2.3. Курсовой проект

Выполнение Курсового проекта является обязательным.

Примерная тематика курсовых проектов

1. Разработка системы защиты информации информационной системы коммерческого предприятия.
2. Анализ внешних угроз сети торгового предприятия.
3. Создание структуры программно-аппаратных средств защиты информации коммерческого предприятия.
4. Защита жесткого диска персонального компьютера от проникновения с помощью программных средств.
5. Защита базы данных предприятия криптографическими методами.
6. Настройка прав пользователей к базам данных коммерческого предприятия.
7. Разработка политики учетных записей коммерческого предприятия.
8. Разработка групповой политики безопасности OS Windows для сотрудников государственного учреждения.
9. Обеспечение сохранности конфиденциальной информации с использованием встроенных в ОС средств защиты.
10. Внедрение программно-аппаратного комплекса в систему защиты организации.
11. Создание защищенной системы предприятия с использованием межсетевых экранов и маршрутизаторов.
12. Обеспечение защиты от вредоносного программного обеспечения и сетевых атак OS Windows с помощью программных средств.
13. Обеспечение целостности данных коммерческого предприятия с помощью резервного копирования.
14. Настройка и конфигурирование средств собственной защиты Windows.
15. Разработка системы защиты информации информационной системы учебного учреждения.
16. Внедрение в сеть организации межсетевого экрана и аппаратного брандмауэра.
17. Построение защищенного VPN между филиалами организации.
18. Построение схемы защиты организации с помощью программно-аппаратных средств.
19. Передача электронной отчетности предприятия с использованием криптографических систем.
20. Построение защиты информации предприятия с помощью шифрования жесткого диска.
21. Шифрование данных предприятия при передаче по сети Интернет.
22. Настройка защиты сервера организации с помощью электронного ключа.
23. Проектирование комплекса программно-аппаратных средств защиты предприятия.
24. Разработка защиты локальной сети с использованием управляемых маршрутизаторов и защиты портов.
25. Использование в системе защиты Монитора безопасности субъекта и Монитора безопасности объекта.
26. Защита информации на серверах с помощью отказоустойчивых томов.
27. Защита сервера базы данных с помощью программно-аппаратных средств.
28. Разработка входа в Информационную систему с использование биометрических параметров.

29. Построение замкнутой информационной системы.

30. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных.

31. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов.

32. Реализация защищенного входа в ОС Windows на базе расширений UEFI.

33. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей.

34. Анализ методов и средств анализа защищенности беспроводных сетей.

35. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.

36. Средства обеспечения информационной безопасности банков данных.

37. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации.

38. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.

39. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа.

40. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации

41. Инструментальные средства анализа рисков информационной безопасности.

42. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Реализация программы предполагает наличие лаборатории программных и программно-аппаратных средств защиты информации.

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

– рабочие места студентов, оборудованные персональными компьютерами;

– лабораторные учебные макеты;

– рабочее место преподавателя;

– учебно-методическое обеспечение модуля;

– доска, комплект презентаций;

– антивирусные программные комплексы;

– программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;

– программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;

– средства уничтожения остаточной информации в запоминающих устройствах;

– программные средства криптографической защиты информации.

3.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, дополнительной литературы, Интернет-ресурсов

1. Бабаш, А. В. Моделирование системы защиты информации. Практикум: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2026. — 355 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01969-6. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2237199 (дата обращения: 11.11.2026)

2. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. — Москва: Издательство Юрайт, 2026. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583783

3. Внуков, А. А. Основы информационной безопасности: защита информации: учебник для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458

4. Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом: учебник для вузов / Е. А. Войниканис; под редакцией М. А. Федотова. — 4-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 50 с. — (Высшее образование). — ISBN 978-5-534-19364-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589232

5. 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, 2026. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст:

электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588246

6. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления: монография / И.С. Клименко. — Москва: ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2238628

7. 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, 2026. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583156

8. Организационное и правовое обеспечение информационной безопасности: учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584372

9. Петровский, М. В. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. - Москва; Вологда: Инфра-Инженерия, 2024. - 144 с. - ISBN 978-5-9729-1610-8. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2169702

10. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2026. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584129

11. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. — Москва: ИНФРА-М, 2026. — 592 с. — (Высшее образование). - ISBN 978-5-16-022294-3. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2261229

12. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2026. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583858

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Образовательное учреждение обеспечивает организацию и проведение текущего контроля и промежуточной аттестации по модулю.

Текущий контроль проводится преподавателем в процессе обучения.

Обучение по профессиональному модулю завершается итоговой аттестацией по модулю в форме квалификационного экзамена.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений. Формы и методы текущего и итогового контроля по профессиональному модулю доводятся до сведения обучающихся не позднее, чем за два месяца от начала обучения.

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	
Итоговая аттестация по модулю - квалификационный экзамен		

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	демонстрация ответственности за принятые решения; обоснованность самоанализа и коррекция результатов собственной работы	
Эффективно взаимодействовать и работать в коллективе и команде	взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	
Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	грамотность устной и письменной речи; ясность формулирования и изложения мыслей	
Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе	соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	

традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения		
Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	
Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик	
Пользоваться профессиональной документацией на государственном и иностранном языках	эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	