Приложение 5
к ППССЗ специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
РЕСПУБЛИКИ ДАГЕСТАН «ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ Р.Н. АШУРАЛИЕВА»

РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА

МДК.02.01. Программные и программно-аппаратные средства защиты информации

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация выпускника: Техник по защите информации

Махачкала 2024 г.

ОДОБРЕНО

предметной (цикловой) комиссией УГС 09.00.00. Информатика и вычислительная техника и 10.00.00 Информационная безопасность

Председатель П(Ц)К

 Ш.М. Мусаева

Протокол №1 от «30» августа 2024 г

Рабочая программа учебной междисциплинарного курса МДК.02.01 Программные и программно-аппаратные средства защиты информации разработана на основе:

- Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации № 1553 от 9 декабря 2016 г., (зарегистрирован Министерством юстиции РФ 26 декабря 2016 г. N 44938);

с учетом:

- Примерной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанной Федеральным учебно-методическим объединением в системе среднего профессионального образования по укрупненным группам профессий и специальностей 10.00.00 Информационная безопасность

в соответствии с рабочим учебным планом по специальности.

Разработчик:

- Полозкова Елена Николаевна, преподаватель ГБПОУ РД «Технический колледж имени Р.Н. Ашуралиева»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ междисциплинарного курса «МДК 02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

1.1. Место междисциплинарного курса в структуре основной профессиональной образовательной программы

Междисциплинарный курс МДК.02.01 Программные и программно-аппаратные средства защиты информации, в составе профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами, принадлежит профессиональному циклу П.00 обязательной части ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Цель и планируемые результаты освоения междисциплинарного курса:

Освоение междисциплинарного курса должно способствовать формированию общих компетенций:

– ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;

– ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

– ОК 03. 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 04. Эффективно взаимодействовать и работать в коллективе и команде.;

– ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

– ОК 06. 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 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

– ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

– ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

Освоение междисциплинарного курса должно способствовать овладению профессиональными компетенциями:

– 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.

В результате освоения междисциплинарного курса обучающийся должен иметь практический опыт:

– установки, настройки программных средств защиты информации в автоматизированной системе;

– 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.

– обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

– использование программных и программно-аппаратных средств для защиты информации в сети;

– решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

– применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных;

– выявления событий и инцидентов безопасности в автоматизированной системе.

В результате освоения междисциплинарного курса обучающийся должен 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;

– 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.

– применять программные и программно-аппаратные средства для защиты информации в базах данных;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– применять средства гарантированного уничтожения информации.

В результате освоения междисциплинарного курса обучающийся должен 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;

– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации.

Общие компетенции:

Код компетенции	**Формулировка компетенции**	**Знания, умения**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
		Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	**Умения:** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
		Знания: номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности

ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; выявлять достоинства и недостатки коммерческой идеи; презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования
		Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде	**Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
		Знания: психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	**Умения:** грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе
		Знания: особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.
ОК 06	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;	**Умения:** описывать значимость своей специальности
		Знания: сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	**Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности
		Знания: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения

ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	**Умения:** использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
		Знания: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

Профессиональные компетенции:

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	**Практический опыт:** Установки, настройки программных средств защиты информации в автоматизированной системе.
	Умения: Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации.
	Знания: Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	**Практический опыт:** Обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами. Использование программных и программно-аппаратных средств для защиты информации в сети.
	Умения: Устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями. Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации.
	Знания: Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных.
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	**Практический опыт:** Тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации.
	Умения: Диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации.
	Знания:

	Методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	**Практический опыт:** Решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации. Применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных
	Умения: Применять программные и программно-аппаратные средства для защиты информации в базах данных. Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации. Применять математический аппарат для выполнения криптографических преобразований. Использовать типовые программные криптографические средства, в том числе электронную подпись.
	Знания: Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных. Типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации. Основные понятия криптографии и типовых криптографических методов и средств защиты информации.
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	**Практический опыт:** Учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности
	Умения: Применять средства гарантированного уничтожения информации.
	Знания: Особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации.
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	**Практический опыт:** Работа с подсистемами регистрации событий. Выявление событий и инцидентов безопасности в автоматизированной системе
	Умения: Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации. Осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
	Знания: Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

2.1. Объем учебной междисциплинарного курса и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы	392
в том числе:	

Урок	94
Лекция	26
Семинар	10
Лабораторные занятия	126
Практические занятия	4
Консультации по курсовому проекту	22
Консультации перед экзаменом	4
Самостоятельная работа	94
Промежуточная аттестация в форме экзамена	12

- Объем времени обязательной части ППССЗ 180 час.
- Объем времени вариативной части ППССЗ 212 час.

По сравнению с примерной программой в рабочей программе междисциплинарного курса количество часов увеличено на 212 часов. Вариативная часть используется на углубление подготовки по междисциплинарному курсу, а также изучения технологии программного комплекса ViPNet и подготовки к демонстрационному экзамену по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

2.2. Тематический план и содержание междисциплинарного курса МДК.02.01 Программные и программно-аппаратные средства защиты информации

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2		3	4
	6 семестр			
Тема 1. Предмет и задачи программно-аппаратной защиты информации	**Лекции**		**4**	ОК 1 – ОК 9, ПК 2.1 - ПК 2.6
	1.	Основные понятия программно-аппаратной защиты информации		
	2.	Классификация методов и средств программно-аппаратной защиты информации		
Тема 2. Стандарты безопасности. Изучение мер защиты информации в информационных системах.	**Лекции**		**4**	
	3.	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами		
	4.	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами		
	Содержание учебного материала		**2**	
	5.	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.		
	Практические занятия		**4**	
	6.	Обзор стандартов. Работа с содержанием стандартов		
	7.	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке		
Тема 3. Защищенная автоматизированная система	**Содержание учебного материала**		8	
	8.	Автоматизация процесса обработки информации. Понятие автоматизированной системы		
	9.	Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении		
	10.	Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС.		
	11.	Дискреционные модели. Мандатные модели		
	Лабораторные работы		14	
	12.	Учет, обработка, хранение и передача информации в АИС.		

	13.	Ограничение доступа на вход в систему		
	14.	Идентификация и аутентификация пользователей. Разграничение доступа		
	15.	Регистрация событий (аудит). Контроль целостности данных.		
	16.	Уничтожение остаточной информации.		
	17.	Управление политикой безопасности. Шаблоны безопасности		
	18.	Криптографическая защита. Обзор программ шифрования данных		
Тема 4. Дестабилизирующее воздействие на объекты защиты	**Содержание учебного материала**		2	
	19.	Источники дестабилизирующего воздействия на объекты защиты. Причины и условия дестабилизирующего воздействия на информацию.		
	Лабораторные работы		2	
	20.	Распределение каналов в соответствии с источниками воздействия на информацию		
Тема 5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание учебного материала**		4	
	21.	Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД		
	22.	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам.		
	Лабораторные работы		4	
	23.	Организация доступа к файлам		
	24.	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД		
Тема 6. Основы защиты автономных автоматизированных систем	**Содержание учебного материала**		6	
	25.	Работа автономной АС в защищенном режиме		
	26.	Алгоритм загрузки ОС		
	27.	Понятие АМДЗ (доверенная загрузка)		
	Лабораторные работы		4	
	28.	Программно-аппаратный комплекс защиты информации «Соболь»		
	29.	Изучение компонентов Программно-аппаратного комплекса защиты информации «Соболь»		
Тема 7. Защита программ и данных от несанкционированного копирования	**Содержание учебного материала**		4	
	30.	Несанкционированное копирование программ как тип НСД		
	31.	Защитные механизмы в современном программном обеспечении на примере MS Office		
	32.	**Лабораторные работы**	6	
	33.	Защита информации от несанкционированного копирования с использованием специализированных программных средств		

	34.	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint). ч.1.		
	35.	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint). ч.2.		
Тема 8. Защита программ от изучения	**Содержание учебного материала**		6	
	36.	Изучение и обратное проектирование ПО		
	37.	Способы изучения ПО: статическое и динамическое изучение. Задачи защиты от изучения и способы их решения		
	38.	Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям		
Тема 9. Вредоносное программное обеспечение	**Содержание учебного материала**		8	
	39.	Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения.		
	40.	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО.		
	41.	Методы обнаружения вредоносного ПО.		
	42.	Классификация антивирусных средств. Сигнатурный и эвристический анализ.		
	Лабораторные работы		12	
	43.	Основные признаки присутствия на компьютере вредоносных программ. Ч.1.		
	44.	Основные признаки присутствия на компьютере вредоносных программ. Ч.2.		
	45.	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО		
	46.	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО		
	47.	Настройка средства антивирусной защиты Kaspersky Endpoint Security 10 для Windows		
	48.	Настройка средств сетевого экранирования Kaspersky Endpoint Security 10 для Windows		
	7 семестр			
Тема 10. Защита информации на машинных носителях	**Лекции**		4	
	49.	Средства восстановления остаточной информации. Создание посекторных образов НЖМД		
	50.	Безвозвратное удаление данных. Принципы и алгоритмы		
	Лабораторные работы		4	
	51.	Применение средства восстановления остаточной информации на примере Foremost или аналога		

	52.	Применение средства безвозвраитного удаления данных File Shredder, WipeFile и аналогов		
Тема 11. Аппаратные средства идентификации и аутентификации пользователей	**Содержание учебного материала**		4	
	53.	ИСПОЛЬЗОВАНИЕ СМАРТ-КАРТ И USB-КЛЮЧЕЙ		
	54.	Устройства Touch Memory		
	Лабораторные работы		6	
	55.	Установка и настройка Rutoken		
	56.	Начало работы с устройствами Рутокен		
	57.	Установка и настройка ключей iButton		
Тема 12. Системы обнаружения атак и вторжений	**Лекции**		6	
	58.	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ.		
	59.	Использование сетевых снифферов в качестве СОВ		
	60.	Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий.		
	Лабораторные работы		20	
	61.	Установка Dallas Lock		
	62.	Настройка системы авторизации пользователей Dallas Lock		
	63.	Настройка прав доступа пользователей к ресурсам в информационной системе, защищенной Dallas Lock		
	64.	Настройка прав доступа пользователей к объектам файловой системы в Dallas Lock		
	65.	Настройка аудита доступа к объектам файловой структуры и внешним устройствам в Dallas Lock		
	66.	Настройка подсистемы очистки остаточной информации в Dallas Lock		
	67.	Использование криптографических методов защиты информации в СЗИ Dallas Lock		
	68.	Контроль целостности программноаппаратной среды защищаемого компьютера в Dallas Lock		
	69.	Настройка замкнутой программной среды в Dallas Lock		
	70.	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений		
Тема 13. Обеспечение безопасности межсетевого взаимодействия	**Лекции**		4	
	71.	Методы защиты информации при работе в сетях общего доступа		
	72.	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall		
	Содержание учебного материала		6	

	73.	Пакетные фильтры. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Proxy-сервера прикладного уровня		
	74.	Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall		
	75.	Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов		
	Лабораторные работы		4	
	76.	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr		
	77.	Изучение различных способов закрытия «опасных» портов		
Тема 14. Средства организации VPN.	**Лекции**		4	
	78.	Виртуальная частная сеть. Функции, назначение, принцип построения		
	79.	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр		
	Лабораторные работы		4	
	80.	Развертывание VPN ч.1		
	81.	Развертывание VPN ч.2		
Тема 15. Мониторинг систем защиты	**Содержание учебного материала**		12	
	82.	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации		
	83.	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25		
	84.	Классификация отслеживаемых событий. Особенности построения систем мониторинга		
	85.	Источники ин0,формации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.		
	86.	Классификация сетевых мониторов		
	87.	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке		
	Лабораторные работы		4	
	88.	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов		
	89.	Проведение аудита ЛВС сетевым сканером		
Тема 16. Система защиты информации «Secret Net»	**Содержание учебного материала**		2	
	90.	Изучение и принцип работы SecretNetStudio		
	Лабораторные работы		10	
	91.	Установка и настройка SecretNetStudio		
	92.	«Secret Net. Разграничение доступа к устройствам		

	93.	«Secret Net. Замкнутая программная среда. Контроль целостности		
	94.	Secret Net. Работа со сведениями в журнале регистрации событий. Теневое копирование		
	95.	Программа оперативного управления. Удаленное управление защищаемым компьютером		
Тема 17. Программно-аппаратный комплекс ViPNet.	**Содержание учебного материала**		36	
	96.	Технология VipNet. Модули защищенной сети VipNet.		
	97.	Объекты защищенной сети VipNet. Межсерверные каналы.		
	98.	Состав и назначение VipNet Administrator.		
	99.	VipNet Policy Manager.		
	100.	Шифрование в технологии Vip Net.Ключевая система VipNet. Компрометация ключей.		
	101.	Программный комплекс «ViPNet Удостоверяющий центр 4».		
	102.	Порядок организации межсетевого взаимодействия		
	103.	Функции ViPNet Coordinator 4.		
		8 семестр		
	104.	Настройка ViPNet Coordinator.		
	105.	Настройка сетевого экрана. Работа с правами администратора.		
	106.	Транспортный модуль ViPNet MFTP. Система обновлений ViPNet.		
	107.	Функции ViPNet Coordinator Linux		
	108.	Созданипе групп и объектов. Сетевые фильтры.		
	109.	Программно-аппаратные комплексы ViPNet Coordinator HW		
	110.	Основные возможности ViPNet Coordinator HW4		
	111.	Система защиты от сбоев.		
	112.	Назначение веб-интерфейса ViPNet Coordinator HW4		
	113.	Командный интерпретатор		
	Лабораторные работы		32	
	114.	Развертывание защищенной сети ViPNet		
	115.	Принципы взаимодействия СУ		
	116.	Режимы работы узлов ViPNet		

	117.	Особенности маршрутизации. Туннелирование. Фильтрация трафика. Антиспуфинг. NAT.		
	118.	Маршрутизация трафика		
	119.	Реализация NAT в координаторе.		
	120.	Установка Координатора.		
	121.	Обзор основных утилит Координатора		
	122.	Базовые параметры координатора.		
	123.	Настройки режимов работы Координатора.		
	124.	Сервер открытого интернета.		
	125.	Установка ПАК Координатор HW.		
	126.	Удаленное управление ПАК.		
	127.	Coordinator Linux. Фильтрация трафика.		
	128.	Coordinator Linux. Настройка автономного режима. Настройка полутуннеля.		
	129.	Coordinator Linux. Настройка кластера горячего резервирования.		
Консультации по курсовому проекту			**22**	
Тематика курсовых проектов 1. Оценка угроз безопасности информации в информационной системе организации при несанкционированном доступе 2. Изучение системы криптографической защиты информации с функцией цифровой подписи 3. Обеспечение защиты информации при передаче по каналам связи, с использованием программно-аппаратных средств защиты 4. Аудит информационной безопасности на примере организации. 5. Анализ методов и средств анализа защищенности беспроводных сетей. 6. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 7. Обеспечения информационной безопасности банков данных при помощи программно-аппарпатных средств.. 8. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса). 9. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации. 10. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота. 11. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа. 12. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации. 13. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела. 14. Инструментальные средства анализа рисков информационной безопасности.				

15. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками. 16. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности). 17. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей. 18. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей 19. Анализ методов и средств анализа защищенности беспроводных сетей 20. Организация обработки персональных данных в компании (организации). 21. Анализ защищенности информационной системы 22. Определение перечня сведений, подлежащих защите в организации 23. Применение системы обнаружение атак и управление рисками 24. Использование электронной цифровой подписи при работе с электронными услугами 25. Методы и средства защиты информации от несанкционированного доступа в сети Интернет			
Консультации перед экзаменом		**4**	
Самостоятельная работа обучающихся:		**94**	
	Изучить теоретический материал и составить тезисы (краткий конспект): – Выполнение курсового проекта – Обзор и анализ современных программно-аппаратных средств защиты информации – Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности – Составление документации по учету, обработке, хранению и передаче конфиденциальной информации – Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации – Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов – Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов – Проблема защиты информации в облачных хранилищах данных и ЦОДах – Сертификация межсетевых экранов – Методические рекомендации ФСТЭК – Настройка программных и программно-аппаратных средств защиты информации		
	Промежуточная аттестация в форме экзамена	**12**	
	Всего	**392**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

3.1. Материально-техническое обеспечение

Для реализации программы междисциплинарного курса МДК.02.01 Программные и программно-аппаратные средства защиты информации, предусмотрена лаборатория Программных и программно-аппаратных средств обеспечения информационной безопасности, оснащенная оборудованием и техническими средствами обучения:

- Рабочие места на 25 обучающихся;
- Автоматизированные рабочие места на 12 обучающихся(. ОЗУ-32ГБ, процессор-11th Gen Intel(R) Core(TM) i7-11700 @ 2.50GHz, 64-разрядная ОС) , подключенные к локальной вычислительной сети и сети «Интернет»;
- Автоматизированное рабочее место преподавателя. ОЗУ-32ГБ, процессор-11th Gen Intel(R) Core(TM) i7-11700 @ 2.50GHz, 64-разрядная ОС;
- Маршрутизаторы MikroTik на 13 рабочих мест.
- Интерактивная доска, проектор, кронштейн;
- МФУ;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения (Microsoft Office, VMware, Oracle VM VirtualBox, AnyDesk, Браузер);
- Антивирусные программные комплексы (Kaspersky Anti-Virus пробная версия);
- Программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности (Aladdin Secret Disk, Secret Net Studio, ViPNet);
- Программные и программно-аппаратные средства обнаружения вторжений (Алладин, Dallas Lock);
- Средства уничтожения остаточной информации в запоминающих устройствах (CBL Data Shredder, PCDiskEraser);
- Программные средства выявления уязвимостей в АС и СВТ (XSpider);
- Программные-аппаратные средства криптографической защиты информации (Рутокен);
- Программные средства защиты среды виртуализации.
- Программно-аппаратный модуль доверенной загрузки «Соболь».
- Комплект учебно-методической документации;
- Фонд оценочных средств по междисциплинарному курсу.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2021. - 248 с.
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с.

3.2.2. Дополнительные печатные источники:

1. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2016
2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2017
3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
6. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
7. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
8. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
9. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
10. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
11. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
13. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
15. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
17. от 30 августа 2002 г. № 282.
18. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

19. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
20. от 31 августа 2010 г. № 416/489.
21. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
22. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
23. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
24. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г.
25. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
26. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
27. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
28. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
29. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
30. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
31. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
32. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
33. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
34. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
35. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

36. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
37. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
38. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
39. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
40. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
41. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
42. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
43. Номенклатура показателей качества. Ростехрегулирование, 2005.
44. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
45. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
46. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
47. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
48. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
49. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
50. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
51. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
52. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
53. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

54. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
55. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
56. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
57. программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;
58. базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

3.2.3. Периодические издания:

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

3.2.3. Электронные источники:

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

3.3. Кадровое обеспечение образовательного процесса

Реализация программы МДК обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых

соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии (имеющих стаж работы в данной профессиональной области не менее 3 лет).

Квалификация педагогических работников должна отвечать квалификационным требованиям, указанным в квалификационных справочниках.

Требования к квалификации педагогических работников. Высшее профессиональное образование или среднее профессиональное образование по направлению подготовки "Образование и педагогика" или в области, соответствующей преподаваемой дисциплине, без предъявления требований к стажу работы, либо высшее профессиональное образование или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности в образовательном учреждении без предъявления требований к стажу работы.

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач
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	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач
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	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач

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	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач
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	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач

Код компетенции	**Формулировка компетенции**	**Знания, умения**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
		Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	**Умения:** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
		Знания: номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности

ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; выявлять достоинства и недостатки коммерческой идеи; презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования
		Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде	**Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
		Знания: психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	**Умения:** грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе
		Знания: особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.
ОК 06	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;	**Умения:** описывать значимость своей специальности
		Знания: сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	**Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности
		Знания: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения

ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	**Умения:** использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
		Знания: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

.