МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Рабочая программа междисциплинарного курса

МДК.03.01Техническая защита информации

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

г. Алексеевка
2023

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Разработчик:

Н.А. Ковалев, преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ
МДК.03.01 Техническая защита информации

1.1. Область применения рабочей программы

Рабочая программа междисциплинарного курса является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения вида деятельности (ВД): Защита информации техническими средствами и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

1.2. Цели и задачи МДК – требования к результатам освоения МДК

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

уметь:

У1 применять технические средства для криптографической защиты информации конфиденциального характера;

У2 применять технические средства для уничтожения информации и носителей информации;

У3 применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

У4 применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

У5 применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

У6 применять инженерно-технические средства физической защиты объектов информатизации.

знать:

З1 порядок технического обслуживания технических средств защиты информации;

З2 номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

З3 физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

З4 порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

З5 методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

З6 номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

З7 основные принципы действия и характеристики технических средств физической защиты;

З8 основные способы физической защиты объектов информатизации;

З9 номенклатуру применяемых средств физической защиты объектов информатизации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции Всероссийского Чемпионата движения по профессиональному мастерству «Профессионалы» по компетенции Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении учебной дисциплины:

1) знать и понимать: типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
2) знать и понимать: каналы передачи данных: определение и виды;

3) знать и понимать: технологии работы с политиками информационной безопасности;

4) уметь: создать объекты защиты и политику ИБ, используя технологии анализа в системе корпоративной защиты;

5) уметь: администрирование автоматизированных технические средства управления и контроля информации и информационных потоков;

6) уметь: создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты.

1.3. Планируемые личностные результаты освоения рабочей программы

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»

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

1.4. Количество часов на освоение рабочей программы МДК:

максимальной учебной нагрузки обучающегося -150 часов, в том числе: аудиторной учебной работы обучающегося - 137 часов, из них в форме практической подготовки – 137 часов; в том числе практических занятий – 69 часов; самостоятельной учебной работы обучающегося - 4 часа; консультаций - 6 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК

Результатом освоения МДК является овладение обучающимися видом деятельности - Защита информации техническими средствами, в том числе общие компетенции (ОК) и профессиональными компетенциями (ПК):

Код	Наименование результата обучения
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, 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	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

3. СТРУКТУРА И СОДЕРЖАНИЕ МДК

3.1. Объем МДК и виды учебной работы

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	150
Аудиторная учебная работа (обязательные учебные занятия) (всего)	150
из них в форме практической подготовки	150
в том числе:	
теоретические занятия	68
лабораторные работы	
практические занятия	69
контрольные работы	
Самостоятельная работа обучающегося (всего)	4
Консультации	6
Промежуточная аттестация в форме ***экзамена***	3

2.2.Тематический план и содержание МДК.03.01 Техническая защита информации

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Коды компетенций (ОК, ПК), личностных результатов (ЛР), умений (У), знаний (З), формированию которых способствует элемент программы
1	2	3	4
МДК.03.01 Техническая защита информации			
Раздел 1. Концепция инженерно-технической защиты информации			
Тема 1.1. Предмет и задачи технической защиты информации	Содержание учебного материала, в том числе в форме практической подготовки	**2/0/2**	ОК1 З1 ЛР 4 ЛР 10
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	**2/0/2**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	*	
	Контрольные работы	*	
Тема 1.2. Общие	Содержание учебного материала, в том числе в форме практической подготовки	**2/0/2**	ОК2

положения защиты информации техническими средствами	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	**2/0/2**	З2 З3 ЛР 4 ЛР 7
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки		
	Контрольные работы	*	
Раздел 2. Теоретические основы инженерно-технической защиты информации			
Тема 2.1. Информация как предмет защиты	Содержание учебного материала, в том числе в форме практической подготовки	**8/2/6**	ОК3 ПК 3.2. З2 У3 ЛР 4 ЛР 9 ЛР 10
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	**8/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/2/2**	
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.		
	Контрольные работы	*	
Тема 2.2. Технические каналы утечки информации	Содержание учебного материала, в том числе в форме практической подготовки	**4/4/8**	ОК5 ПК 3.1. З3 У1 ЛР 4 ЛР 9 ЛР 10
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/4/4**	
	Классификация демаскирующих признаков. Основные виду угроз информации Обоснование выбора кабинета как объекта защиты. Составление плана кабинета как объекта		

	защиты		
	Контрольные работы	*	
Тема 2.3. Методы и средства технической разведки	Содержание учебного материала, в том числе в форме практической подготовки	**4/2/6**	ОК9 ПК3.2. ПК3.3. З4 З5 У4 ЛР 4 ЛР 9 ЛР 10
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/2/2**	
	Типовая структура технических каналов утечки. Моделирование каналов утечки информации Методы добывания информации о вещественных носителях		
	Контрольные работы	*	
Раздел 3. Физические основы технической защиты информации			
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание учебного материала, в том числе в форме практической подготовки	**4/4/8**	ОК10 ПК3.2. ПК3.3. З4 З5 У4 ЛР 4
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/4/4**	
	Измерение параметров физических полей		
	Контрольные работы	*	
Тема 3.2. Физические процессы при подавлении опасных сигналов	Содержание учебного материала, в том числе в форме практической подготовки	**4/4/8**	ОК1 ПК3.2. ПК3.3. З7 У4
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/4/4**	

	Защита аппаратуры от электромагнитных полей		ЛР 4
	Контрольные работы	*	
Раздел 4. Системы защиты от утечки информации			
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание учебного материала, в том числе в форме практической подготовки	**4/4/8**	ОК2 ПК 3.4. З6 У4 ЛР 4
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/4/4**	
	Защита от утечки по акустическому каналу		
	Контрольные работы	*	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	Содержание учебного материала, в том числе в форме практической подготовки	**4/4/8**	ОК3 ПК 3.4. З8 У6 ЛР 4 ЛР 7
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/4/4**	
	Системы защиты от утечки информации по проводному каналу		
	Контрольные работы	*	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	Содержание учебного материала, в том числе в форме практической подготовки	**4/4/8**	ОК5 ПК 3.4. З8 У6 ЛР 4 ЛР 7 ЛР 10
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/4/4**	

	Защита от утечки по виброакустическому каналу		
	Контрольные работы	*	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание учебного материала, в том числе в форме практической подготовки	**4/7/11**	ОК5 ПК 3.4. З8 З6 У5 ЛР 10 ЛР 11
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/7/7**	
	Определение каналов утечки ПЭМИН		
	Защита от утечки по цепям электропитания и заземления		
	Контрольные работы	*	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание учебного материала, в том числе в форме практической подготовки	**4/4/8**	ОК10 ПК 3.5. У4 З9 ЛР 4 ЛР 10 ЛР 11
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/4/4**	
	Технические средства защиты информации в телефонных линиях		
	Контрольные работы	*	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Содержание учебного материала, в том числе в форме практической подготовки	**4/4/8**	ОК10 ПК 3.5. З9 У4 ЛР 4
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	**4/0/4**	
	Лабораторные занятия	*	

	Практические занятия, в том числе в форме практической подготовки	**0/4/4**	ЛР 10
	Системы защиты от утечки информации по электросетевому каналу		
	Контрольные работы	*	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	Содержание учебного материала, в том числе в форме практической подготовки	**4/4/8**	ОК5 ПК 3.5. З8 У6 ЛР 4 ЛР 7 ЛР 9-11
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/4/4**	
	Системы защиты от утечки информации по оптическому каналу		
	Контрольные работы	*	
Раздел 5. Применение и эксплуатация технических средств защиты информации			
Тема 5.1. Применение технических средств защиты информации	Содержание учебного материала, в том числе в форме практической подготовки	**4/14/18**	ОК10 ПК 3.5. У4 З7 ЛР 4 ЛР 7 ЛР 9-11
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	**4/0/4**	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/14/14**	
	Применение технических средств защиты Представление моделей объектов информационной безопасности Определение путей проникновения злоумышленника к источнику информации Типовые индикаторы каналов утечки Комплексная система защиты		
	Контрольные работы	*	
Тема 5.2.	Содержание учебного материала, в том числе в форме практической подготовки	**8/8/16**	ОК10

Эксплуатация технических средств защиты информации	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	**8/0/8**	ПК 3.2. ЛР 4 ЛР 7 ЛР 9-11
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**0/10/8**	
	Эксплуатация технических средств защиты Комплексы обнаружения и пеленгации Анализаторы телефонных линий Гарантированное уничтожение информации на магнитных носителях		
	Контрольные работы	*	
Самостоятельная работа обучающихся	1. Подготовка информационного сообщения на тему: «Основные проблемы реализации систем защиты информации» 2. Поиск информации по теме: «Биометрическая идентификация»	**4**	
	Консультации	**6**	
Экзамен		**3**	
	Всего:	**150**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК

4.1. Требования к минимальному материально-техническому обеспечению:

Реализация рабочей программы МДК предполагает наличие лаборатории технических средств защиты информации - 65,4 кв.м.

Оборудование учебного кабинета: доска, 15 автоматизированных рабочих мест для студентов: столы-15 шт., стулья -15 шт., ПК-15 шт., автоматизированное рабочее место для преподавателя – 1 шт., сканер-1 шт., принтер-1 шт., проектор – 1шт., экран – 1 шт.; программное обеспечение общего и профессионального назначения, лабораторные учебные макеты.

Основное оборудование: учебно-методическая документация; аппаратные средства аутентификации пользователя.

лекционной аудитории с мультимедийным оборудованием - 11,8 кв.м.

Оборудование учебного кабинета: доска – 1 шт., шкаф – 4 шт., 32 посадочных места для студентов (32 стула, 16 столов), рабочее место преподавателя – 1 шт., телевизор «Sony» - 1 шт; интерактивная доска – 1шт.; мультимедийный проектор «Acer» - 1 шт, компьютер – 1шт., принтер – 1 шт.

Основное оборудование: стенды «Техника безопасности», «Уголок группы», «Сегодня на учебном занятии», «Лучшие работы студентов», комплект учебно-методической документации.

Демонстрационные средства обучения:раздаточный материал для проведения учебных занятий по дисциплине, набор презентаций и видеоматериалов.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение обучения

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Технические средства информатизации. Учебник для СПО/ Е. И. Гребенюк, Н. А. Гребенюк М.: ИЦ Академия,2019 – 352 с.

2. Технические средства информатизации: учебник/ Гагарина Л.Г. - М.: ИД Форум, 2023.-256 с.

Дополнительные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015
3. Новиков В.К. Организационное и правовое обеспечение информационнойбезопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013 – 172 с.
4. Организационно-правовое обеспечениеИнформационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов,В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017 – 336с
5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие -Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации Академия, - 336 с. – 2012
7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд во: ДМК Пресс, - 2012
8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012 – 416 с.
9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
13. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
14. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

15. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
16. 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».
17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
18. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
19. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
20. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
21. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
22. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
23. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
24. от 30 августа 2002 г. № 282.
25. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
26. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
27. от 31 августа 2010 г. № 416/489.

28. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
29. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
30. 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.
31. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
32. 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
33. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
34. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
35. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
36. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
37. 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
38. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
39. 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

40. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
41. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
42. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
43. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
44. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
45. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
48. Номенклатура показателей качества. Ростехрегулирование, 2005.
49. 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.
50. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
51. 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.
52. 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.

53. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
54. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
55. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.
56. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
57. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
58. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.
59. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
60. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
61. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Электронные издания (электронные ресурсы):

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.
2. https://urait.ru/bcode/456793
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, 2020. — 312 с.
4. https://urait.ru/bcode/449548
5. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального

образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с.
6. https://urait.ru/bcode/451933
7. Интерфейсы периферийных устройств – https://intuit.ru/studies/courses/92/92/lecture/28396
8. О компонентах системного блока — подробно – https://intuit.ru/studies/courses/3685/927/lecture/19564?page=2
9. Портативные компьютеры – https://intuit.ru/studies/courses/13910/1276/lecture/24146
10. Сравнительные характеристики процессоров – https://intuit.ru/studies/courses/15812/478/lecture/21074
11. Технические средства информационных технологий – https://intuit.ru/studies/courses/3481/723/lecture/14240
12. Устройства ввода информации – https://intuit.ru/studies/courses/3460/702/lecture/14158
13. Устройства вывода информации – https://intuit.ru/studies/courses/3460/702/lecture/14157
14. Цифровая образовательная среда СПО PROFобразование:
- Старостин, А. А. Технические средства автоматизации и управления : учебное пособие для СПО / А. А. Старостин, А. В. Лаптева ; под редакцией Ю. Н. Чеснокова. — 2-е изд. — Саратов, Екатеринбург : Профобразование, Уральский федеральный университет, 2019. — 168 с. — ISBN 978-5-4488-0503-5, 978-5-7996-2842-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87882 (дата обращения: 31.08.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:
IPRBOOKS - http://www.iprbookshop.ru/78574.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК

Контроль и оценка результатов освоения МДК осуществляется преподавателем в процессе проведения теоретических и практических занятий, экзамена.

Результаты (освоенные профессиональные компетенции)с учетом личностных результатов, профессионального стандарта и стандарта компетенции Ворлдскиллс	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке ипроведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике Экзамен
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	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 Экзамен

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	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 Экзамен
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	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 Экзамен
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	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 Экзамен