

Приложение
к ОПОП по специальности
10.02.05 Обеспечение
информационной безопасности
автоматизированных систем

Рабочая программа профессионального модуля

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

**по специальности
среднего профессионального образования
(программа подготовки специалистов среднего звена)**

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Омск, 2025 г.

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

1.1. Область применения программы

Рабочая программа профессионального модуля «Защита информации техническими средствами» является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля

Целями освоения профессионального модуля являются:

- изучение и практическое освоение основ инженерно-технической защиты информации как составной части системы защиты информации;
- изучение и практическое освоение технических средств охраны как составной части системы защиты информации.

Задачами освоения профессионального модуля являются:

- изучение обучающимися методов и способов инженерно-технической защиты информации от утечки по техническим каналам, несанкционированного и непреднамеренного воздействия на информацию, проведения организационно-технических и технических мероприятий по защите информации, организации контроля за эффективностью создаваемых систем защиты.
- изучение обучающимися технических средств, используемых для охраны объектов и помещений, методик определения необходимого уровня физической безопасности объекта, принципов построения систем охраны с помощью технических средств, основных параметров технических средств охраны.

В результате освоения дисциплины обучающийся должен:

Иметь практический опыт	– установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов
-------------------------	--

	информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.
уметь	– применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации
знать	– порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися основным видом деятельности (ВД) Защита информации техническими средствами, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля ПМ.03 Защита информации техническими средствами

Индекс	Наименование циклов, дисциплин, профессиональных модулей, МДК, практик	Объем образовательной программы (всего)	в т.ч. в форме практической подготовки	Учебная нагрузка обучающегося (час.)						
				самостоятельная работа	во взаимодействии с преподавателем					
					в том числе					промежуточная аттестация
					всего	лекции	практические, лабораторные занятия, семинары	курсовые проекты (работы)	консультации	
ПМ.03	Защита информации техническими средствами	572	164	114	288	80	164	24	20	26
МДК.03.01	Техническая защита информации	130	58	38	90	26	58	0	6	2
МДК.03.02	Инженерно-технические средства физической защиты объектов информатизации	190	66	50	128	30	66	24	8	12
МДК.03.03	Корпоративная защита от внутренних угроз информационной безопасности	108	40	26	70	24	40	0	6	12
УП.03	Учебная практика	36								
ПП.03	Производственная практика	108								

3.2. Тематический план и содержание профессионального модуля

3.2.1 Тематический план и содержание МДК.03.01 Техническая защита информации

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	130
аудиторная учебная нагрузка (всего):	
лекций	26
практических занятий,	58
включая курсовую работу	-
консультации	6
Промежуточная аттестация	2
Самостоятельная работа обучающегося	38
Промежуточная аттестация в форме зачета с оценкой	

№ п/п	Тема	Количество часов						
		Всего	Лекции	Практические занятия	Курсовая работа	Консультации	СРС	Промежуточная аттестация
1.	Тема 1.1. Предмет и задачи технической защиты информации	2	2					
2.	Тема 1.2. Общие положения защиты информации техническими средствами	2	2					
3.	Тема 2.1. Информация как предмет защиты	8	2	4			2	
4.	Тема 2.2. Технические каналы утечки информации	10	2	4			4	
5.	Тема 2.3. Методы и средства технической разведки	10	2	4			4	
6.	Тема 3.1. Физические основы утечки информации по каналам	8		4			4	
7.	Тема 3.2. Физические процессы при подавлении опасных сигналов	8		4			4	
8.	Консультация	2				2		
	За семестр	50	10	20		2	18	
9.	Тема 4.1. Системы защиты от утечки информации по акустическому каналу	8	2	4			2	
10.	Тема 4.2. Системы защиты от утечки информации по проводному каналу	8	2	4			2	
11.	Тема 4.3. Системы защиты от	8	2	4			2	

	утечки информации по вибрационному каналу							
12.	Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	8	2	4			2	
13.	Консультация	2				2		
14.	Тема 4.5. Системы защиты от утечки информации по телефонному каналу	10	2	4			4	
15.	Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	8	2	4			2	
16.	Тема 4.7. Системы защиты от утечки информации по оптическому каналу	8	2	4			2	
17.	Тема 5.1. Применение технических средств защиты информации	8	2	4			2	
18.	Тема 5.2. Эксплуатация технических средств защиты информации	8		6			2	
19.	Консультация	2				2		
20.	Промежуточная аттестация	2						2
	За семестр	80	16	38		4	20	2
	ВСЕГО	130	26	58		6	38	2

Раздел 1. Концепция инженерно-технической защиты информации

Тема 1.1. Предмет и задачи технической защиты информации

Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.

Системный подход при решении задач инженерно-технической защиты информации.

Основные параметры системы защиты информации.

Тема 1.2. Общие положения защиты информации техническими средствами

Задачи и требования к способам и средствам защиты информации техническими средствами.

Принципы системного анализа проблем инженерно-технической защиты информации.

Классификация способов и средств защиты информации.

Раздел 2. Теоретические основы инженерно-технической защиты информации

Тема 2.1. Информация как предмет защиты

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. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.

Тема 2.2. Технические каналы утечки информации

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.

Классификация демаскирующих признаков Основные виды угроз информации
Обоснование выбора кабинета как объекта защиты
Составление плана кабинета как объекта защиты

Тема 2.3. Методы и средства технической разведки

Классификация технических средств разведки. Методы и средства технической разведки.

Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.

Типовая структура технических каналов утечки

Моделирование каналов утечки информации

Методы добывания информации о вещественных носителях

Дистанционный анализ веществ

Раздел 3. Физические основы технической защиты информации

Тема 3.1. Физические основы утечки информации

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 излучений и наводок аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей

Измерение параметров физических полей

Тема 3.2. Физические процессы при подавлении опасных сигналов

Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.

Изучение физических процессов при подавлении опасных сигналов

Раздел 4. Системы защиты от утечки информации

Тема 4.1. Системы защиты от утечки информации по акустическому каналу

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.

Защита от утечки по акустическому каналу

Энергетическое скрытие акустических сигналов: звукоизоляция и звукопоглощение

Тема 4.2. Системы защиты от утечки информации по проводному каналу

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.

Работа остронаправленных микрофонов

Работа диктофонов со скрытой записью

Тема 4.3. Системы защиты от утечки информации по вибрационному каналу

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.

Защита от утечки по виброакустическому каналу.

Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу

Прослушивание информации от радиотелефонов. Прослушивание информации от работающей

аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации от пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.

Определение каналов утечки ПЭМИН.

Защита от утечки по цепям электропитания и заземления.

Тема 4.5. Системы защиты от утечки информации по телефонному каналу

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.

Работа скремблеров и вокодеров.

Тема 4.6. Системы защиты от утечки информации по электросетевому каналу

Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.

Активное подавление сигналов радиолокаторов.

Защита от утечки информации по электросетевому каналу.

Тема 4.7. Системы защиты от утечки информации по оптическому каналу

Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.

Маскировка в видимом и ИК диапазонах света.

Способы и средства видеоконтроля.

Раздел 5. Применение и эксплуатация технических средств защиты информации

Тема 5.1. Применение технических средств защиты информации

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.

Представление моделей объектов информационной безопасности.

Определение путей проникновения злоумышленника к источнику информации. Типовые индикаторы каналов утечки.

Комплексная система защиты.

Тема 5.2. 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.

Комплексы обнаружения и пеленгации.

Анализаторы телефонных линий.

Гарантированное уничтожение информации на магнитных носителях.

3.2.2 Тематический план и содержание МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	190
аудиторная учебная нагрузка (всего):	
лекций	30
практических занятий,	66
включая курсовую работу	24
консультации	8
Промежуточная аттестация	12
Самостоятельная работа обучающегося	50
Промежуточная аттестация в форме экзамена	

№ п/п	Тема	Количество часов						
		Всего	Лекции	Практические занятия	Курсовая работа	Консультации	СРС	Промежуточная аттестация
1.	Тема 1.1. Цели и задачи физической защиты объектов информатизации	10	4	2			4	
2.	Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	12	6	2			4	
3.	Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	14	2	8			4	
4.	Тема 2.2. Система контроля и управления доступом	14	2	8			4	
5.	Консультация	2				2		
	За семестр	52	14	20		2	16	
6.	Тема 2.3. Система телевизионного наблюдения	20	4	10			6	
7.	Курсовая работа	6			6			
8.	Тема 2.4. Система сбора, обработки, отображения и документирования информации	16	2	8			6	
9.	Консультация	2				2		
10.	Тема 2.5 Система воздействия	16	2	8			6	
11.	Курсовая работа	6			6			
12.	Тема 3.1 Применение инженерно-технических средств физической защиты	20	4	10			6	
13.	Курсовая работа	6			6			
14.	Тема 3.2. Эксплуатация инженерно-	20	4	10			6	

	технических средств физической защиты							
15.	Курсовая работа	6			6			
16.	Консультация	2				2		
17.	Промежуточная аттестация	12						12
	За семестр	138	16	46	24	6	34	12
	ВСЕГО	190	30	66	24	8	50	12

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты

Тема 1.1. Цели и задачи физической защиты объектов информатизации

Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.

Классификация демаскирующих признаков.

Обоснование выбора кабинета как объекта защиты. Составление плана кабинета как объекта защиты.

Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.

Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты
Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.

Типовые инженерные конструкции. Исследование систем охраны.

Способы и средства обнаружения злоумышленников и пожара.

Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты

Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты

Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.

Монтаж датчиков пожарной и охранной сигнализации

Тема 2.2. Система контроля и управления доступом

Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.

Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя

Рассмотрение принципов устройства, работы и применения средств контроля доступа

Тема 2.3. Система телевизионного наблюдения

Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы.

Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.
Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.

Тема 2.4. Система сбора, обработки, отображения и документирования информации
Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.
Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.

Тема 2.5 Система воздействия

Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.

Исследование технических средств воздействия.

Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты

Тема 3.1 Применение инженерно-технических средств физической защиты

Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.

Представление моделей объектов информационной безопасности.

Определение путей проникновения злоумышленника к источнику информации.

Тема 3.2. Эксплуатация инженерно-технических средств физической защиты

Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.

Изучение принципов диагностики, устранения отказов и восстановления работоспособности технических средств физической защиты.

Примерная тематика курсового проекта (работы)

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

11. Расчет системы безопасности и контроля доступа коммерческой организации.
12. Моделирование объекта защиты и угроз безопасности информации для некоммерческой организации.
13. Расчет системы безопасности и контроля доступа производственного здания.
14. Комплексная система безопасности информации коммерческой организации.
15. Моделирование объекта защиты и угроз безопасности информации.

3.2.3 Тематический план и содержание МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	108
аудиторная учебная нагрузка (всего):	
лекций	24
практических занятий,	40
включая курсовую работу	
консультации	6
Промежуточная аттестация	12
Самостоятельная работа обучающегося	26
Промежуточная аттестация в форме экзамена	

№ п/п	Тема	Количество часов						
		Всего	Лекции	Практические занятия	Курсовая работа	Консультации	СРС	Промежуточная аттестация
1.	Тема 1.1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	14	4	6			4	
2.	Тема 1.2. Отчетность и нормативно-правовое обеспечение корпоративной безопасности	14	4	6			4	
3.	Консультация	2				2		
4.	Тема 1.3 Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	18	4	8			6	
5.	Тема 1.4. Технологии защиты и анализа сетевого трафика	14	4	6			4	
6.	Консультация	2				2		
7.	Тема 1.5. Технологии защиты узла и агентского мониторинга	14	4	6			4	
8.	Тема 1.6. Предотвращение инцидентов и управление событиями информационной безопасности	16	4	8			4	
9.	Консультация	2				2		
10.	Промежуточная аттестация	12						12
	ВСЕГО	108	24	40		6	26	12

3.2.4 Учебная практика

Виды работ:

1. Измерение параметров физических полей.
2. Определение каналов утечки ПЭМИН.
3. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.
4. Установка и настройка технических средств защиты информации.
5. Проведение измерений параметров побочных электромагнитных излучений и наводок.
6. Проведение аттестации объектов информатизации.
7. Монтаж различных типов датчиков.
8. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.
9. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.
10. Рассмотрение системы контроля и управления доступом.
11. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.
12. Рассмотрение датчиков периметра, их принципов работы.
13. Выполнение звукоизоляции помещений системы шумления.
14. Реализация защиты от утечки по цепям электропитания и заземления.
15. Разработка организационных и технических мероприятий по заданию преподавателя;
16. Разработка основной документации по инженерно-технической защите информации.

3.2.5 Производственная практика профессионального модуля

Виды работ

1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации.
2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.
3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съема и утечки по техническим каналам.
4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.
5. Изучение порядка применения нормативных правовых актов.
6. Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами.
7. Выявление технических каналов утечки информации.
8. Применение существующих способов выявления опасности целостности информации.
9. Анализ объектов информатизации предприятий, учреждений, организаций.
10. Анализ ресурсов обеспечения инженерно-технической защиты информации.
11. Изучение основных этапов проектирования системы защиты информации техническими средствами.
12. Проектирование рабочих проектов по системам пожарно-охранной сигнализации, видеонаблюдения, СКУД.
13. Оформление технической и технологической документации.

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения: кабинет информационной безопасности, лаборатория технических средств защиты информации, компьютерный класс.

Оборудование и технические средства обучения кабинета информационной безопасности:

Посадочные места для обучающихся

Рабочее место преподавателя

Мультимедийный проектор, экран

Оснащение лаборатории технических средств защиты информации:

Антенна дипольная активная ВЧ АИ5-0

Анализатор спектра FS300

Калибратор акустический в комплекте SV 30A

Анализатор проводных коммуникаций ULAN 2

Комплекс для проведения акустических измерений

Локаатор нелинейный "Катран"

Комплекс оценки эффективности защиты речевой информации от утечки по акустическим и акустоэлектрическим каналам "Колибри"

Генератор виброакустический

Приемник сканирующий

Радиокамера ночного наблюдения

Телевизор Samsung-25

Паяльник 40Вт/220В

Виброизлучатель

Аудиоизлучатель

Генератор шума "Соната-РК1"

Блокиратор сотовых телефонов ЛГШ-701

Рабочая станция (Pentium) 1 шт.

Проектор, экран

Аппаратное средство аутентификации пользователей – ПКЗИ "ШИПКА", ключевой носитель eToken, Guardant Armor, Guardant SP

Средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок – "Соната-АВ" модель 1М и Генератор шума Гном-3

Средство измерения параметров физических полей (в т.ч. электромагнитных излучений и наводок, акустических (виброакустических) колебаний) – Анализатор спектра Rohde & Schwarz FS300; комплекс «КОЛИБРИ»;

Шумомер, виброметр SVAN-947.

Стенды физической защиты объектов информатизации, оснащенными СКД, системами видеонаблюдения и охраны объектов – стенд на основе прибора приемно-контрольного

«Гранит-4», стенд для изучения системы КУД с электромеханическим замком ПОЛИС, RF- камера Wireless 1.2GHz RF 12-IR Night-Vision и веб-камера.

4.2. Информационное обеспечение обучения

Основная литература:

Белов, Е. Б. Организационно-правовое обеспечение информационной безопасности : учебник. Рек. ФУМО СПО ИБ / Е. Б. Белов, В. Н. Пржегорлинский .— М. : Издат. центр "Академия", 2020 .— 336 с.

Дополнительная литература:

Бубнов, А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник. Рек. ФУМО / А. А. Бубнов, В. Н. Пржегорлинский, К. Ю. Фомина

.— М. : Издат. Центр «Академия», 2019 .— 272 с.

Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=429070>

Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова ; Министерство образования и науки Российской Федерации, Оренбургский Государственный Университет, Кафедра вычислительной техники и защиты информации– Оренбург : Оренбургский государственный университет, 2017. – 158 с. : табл., схем. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=481730>

Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие

: [16+] / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: <http://biblioclub.ru/index.php?page=book&id=480636>

Периодические издания:

Вестник	информационной	безопасности
https://dlib.eastview.com/browse/publication/84979	Вопросы	защиты
https://dlib.eastview.com/browse/publication/93931	Информационная	безопасность
https://dlib.eastview.com/browse/publication/90269		

Электронные источники:

Федеральная служба по техническому и экспортному контролю <https://fstec.ru/>
Информационный портал по безопасности <https://www.securitylab.ru/> Федеральный портал «Российское образование» <https://edu.ru/>

Справочно-правовая система «КонсультантПлюс»

4.3. Общие требования к организации образовательного процесса

В преподавании дисциплины используются следующие образовательные технологии: лекции; лабораторный практикум. В активной и интерактивной форме проводятся следующие занятия:

Интерактивные лекции-консультации;

Интерактивные проблемные лекции;

Интерактивные практические занятия-семинары в форме деловой игры;
Компьютерные симуляции;

Разбор конкретных практических ситуаций; Психологические и иные тренинги.

Лабораторный практикум так же является интерактивной формой проведения занятий, поскольку во время таких занятий происходит постоянное взаимодействие по каналам педагогических коммуникаций преподаватель <=> студент и студент <=> студент. При организации образовательного процесса, в условиях реализации компетентностного подхода предусматривается использование активных форм проведения занятий, в том числе может быть реализовано с применением электронного обучения и дистанционных образовательных технологий. Кроме того, в процессе преподавания дисциплины используются следующие образовательные технологии:

- выполнение заданий под руководством преподавателя в компьютерном классе

(форма занятия – лабораторные занятия);

- мозговой штурм (интерактивная методика) (форма занятия – лекция);
 - обмен опытом (форма занятия – лекция);
 - наглядная демонстрация (форма занятия – лабораторные занятия);
 - обсуждение конкретных ситуаций (интерактивная методика) (форма занятия – лабораторные занятия);
 - работа в группах (workshops) (интерактивная методика) (форма занятия – лабораторные занятия);
 - обсуждение критического явления (интерактивная методика) (форма занятия – лекция).
- Внеаудиторная работа обучающихся предполагает вопросы, тематические эссе, аналитическую обработку отчетов, составление расчетно-аналитических таблиц, подготовку сообщений к выступлению на семинаре, подготовку докладов.

Кроме того, что обучающихся в рамках самостоятельной внеаудиторной работы для овладения знаниями должны осуществлять чтение текстов (учебника и дополнительной литературы), составление плана текста, конспектирование текстов, делать необходимые выписки, работать со словарями и справочниками, знакомится и изучать нормативные документы; для закрепления и систематизации знаний должны работать с конспектами лекций, отвечать на контрольные вопросы, осуществлять аналитическую обработку текстов (аннотирование, рецензирование, реферирование, контент-анализ); для формирования умений студенты должны решать задачи.

Практическая подготовка организуется в учебных и структурных подразделениях колледжа, а также в специально оборудованных помещениях (рабочих местах) профильной организации на основании договора о практической подготовке обучающихся № 5 от 22 сентября 2020 г. с федеральным государственным образовательным учреждением высшего образования «Сибирский государственный автомобильно-дорожный университет (СибАДИ)».

4.4. Кадровое обеспечение образовательного процесса

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, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности, в общем числе педагогических работников, реализующих образовательную программу, должна быть не менее 25 процентов.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты (освоенные профессиональные компетенции)	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 и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	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
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
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

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 по квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
---	--	--

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Код и наименование общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	– обоснованность постановки цели, выбора и применения методов, и способов решения профессиональных задач; адекватная оценка деятельности самооценка эффективности выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 02. Использовать современные средства поиска, анализа информации, интерпретации информации, информационные технологии для выполнения задач профессиональной деятельности	– использование различных источников, включая электронные ресурсы, медиа ресурсы, Интернет- ресурсы, периодические издания по специальности для решения профессиональных задач	Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам
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	– демонстрация ответственности за принятые решения – обоснованность самоанализа и коррекция результатов собственной работы; – определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования	Экзамен по модулю
ОК 04. Эффективно взаимодействовать и работать в	– взаимодействие с обучающимися,	

коллективе и команде	преподавателями в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	- грамотность устной и письменной речи, ясность формулирования и изложения мыслей	
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	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	- эффективность использования профессиональной деятельности необходимой технической документации, в том числе на иностранном языке.	