



Негосударственное частное учреждение
Профессиональная образовательная организация
«Уральский институт подготовки кадров «21-й век»

УТВЕРЖДАЮ:

Председатель учебно-методического
совета

заместитель директора

М.В. Федорук

« 04 » августа 2018 г.

Программа профессионального модуля
ПМ.01 Участие в планировании и организации работ
по обеспечению защиты объекта

по специальности

10.02.01 Организация и технология защиты информации

Нижний Тагил

2018 г.

Рабочая программа профессионального модуля разработана на основе
Федерального государственного образовательного стандарта по
специальности среднего профессионального образования
10.02.01 Организация и технология защиты информации

Организация-разработчик НЧУ ПОО «Уральский институт подготовки
кадров «21-й век»

Составитель: Куликов Ю.А. преподаватель кафедры Информационных
технологий, к.м.н.

Программа рассмотрена и утверждена на заседании кафедры
Информационных технологий

«3» августа 2018 г. протокол № 1

Зав. кафедрой  А.А. Трепалин

СОДЕРЖАНИЕ

	стр
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	9
УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	34
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	37

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 090905 Организация и технология защиты информации, входящей в укрупненную группу специальностей 090000 Информационная безопасность, в части освоения основного вида профессиональной деятельности (ВПД): Участие в планировании и организации работ по обеспечению защиты объекта и соответствующих профессиональных компетенций (ПК):

ПК 1.1 Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации

ПК 1.2 Применять программно-аппаратные и инженерно-технические средства защиты информации на объектах профессиональной деятельности

ПК 1.3 Участвовать в эксплуатации защищенных объектов

ПК 1.4 Проводить регламентные работы и фиксировать отказы средств защиты. Выявлять и анализировать возможные угрозы информационной безопасности объектов

ПК 1.5 Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации

ПК 1.6 Обеспечить технику безопасности при проведении организационно-технических мероприятий

ПК 1.7 Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите

ПК 1.8 Проводит контроль за соблюдением персоналом требований режима по защите информации

ПК 1.9 Участвовать в оценке качества защиты объекта

1.2. ЦЕЛИ И ЗАДАЧИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ - ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

С целью овладения профессионального модуля и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен: иметь практический опыт:

- использования физических средств защиты объекта;
- применения физических средств контроля доступа на объект;
- ведения текущей работы исполнителей с конфиденциальной информацией

уметь:

- организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;
- пользоваться аппаратурой систем контроля доступа;
- выделять зоны доступа по типу и степени конфиденциальности работ;
- определять порядок организации и проведения рабочих совещаний;
- использовать методы защиты информации в рекламной и выставочной деятельности;
- использовать критерии подбора и расстановки сотрудников подразделений защиты информации;
- организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
- проводить инструктаж персонала по организации работы с конфиденциальной информацией;
- контролировать соблюдение персоналом требований режима защиты информации;

знать:

- виды и способы охраны объекта;
- особенности охраны персонала организации;
- основные направления и методы организации режима и охраны объекта;
- разрешительную систему доступа к конфиденциальной информации;
- принципы действия аппаратуры систем контроля доступа;
- принципы построения и функционирования биометрических систем безопасности;
- требования и особенности оборудования режимных помещений;
- требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров;
- требования режима защиты информации при приеме в организации посетителей;
- организацию работы при осуществлении международного сотрудничества;
- требования режима защиты информации в процессе рекламной деятельности;
- требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;
- задачи, функции и структуру подразделений защиты информации;
- принципы, методы и технологию управления подразделений защиты информации;
- порядок оформления допуска лиц к конфиденциальным сведениям;
- методы проверки персонала по защите информации;

- процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.

- 1.3. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

максимальной учебной нагрузки обучающегося - 720 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося - 90 часа;

самостоятельной работы обучающегося - 342 часов;

учебная практика – 144 часа

производственная практика по профилю специальности - 144 часа

Формой аттестации по профессиональному модулю являются:

МДК.01.01 Обеспечение организации системы безопасности
предприятия:

зачет – 3 семестр, экзамен – 4 семестр;

МДК.01.02 Организация работ подразделений защиты информации:

зачет – 3, 4 семестр,

МДК.01.03 Организация работы персонала с конфиденциальной
информацией:

зачет – 3, 4 семестр.

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности Участие в планировании и организации работ по обеспечению защиты объекта, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 1.1.	Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации
ПК 1.2.	Применять программно-аппаратные и инженерно-технические средства защиты информации на объектах профессиональной деятельности
ПК 1.3.	Участвовать в эксплуатации защищенных объектов
ПК 1.4.	Проводить регламентные работы и фиксировать отказы средств защиты. Выявлять и анализировать возможные угрозы информационной безопасности объектов
ПК 1.5.	Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации
ПК 1.6.	Обеспечить технику безопасности при проведения организационно- технических мероприятий
ПК 1.7.	Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите
ПК 1.8.	Проводит контроль за соблюдением персоналом требований режима по защите информации
ПК 1.9.	Участвовать в оценки качества защиты объекта
ОК1.	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности
ОК 10.	Применять математический аппарат для решения различных задач.

ОК 11	Оценивать значимость документов, применяемых в профессиональной деятельности.
ОК 12.	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
3.1. ТЕМАТИЧЕСКИЙ ПЛАН ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Коды ПК	Наименования разделов ПМ	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика		
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности)	
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов			
1	2	3	4	5	6	7	8	9	10	
ПК 1.1. ПК 1.2 ПК 1.3. ПК 1.4.	МДК.01.01 Обеспечение организации системы безопасности предприятия	144	30	20		114	-	-	-	
ПК 1.6. ПК 1.7.	МДК.01.02 Организация работ подразделений защиты информации	144	30	20		114				
ПК 1.5. ПК 1.8. ПК 1.9.	МДК.01.03 Организация работы персонала с конфиденциальной	144	30	20		114				
ПК 1.1- ПК1.9	Учебная практика	144						144		
ПК 1.1- ПК1.9	Производственная практика (по профилю специальности)	144								144
	Всего:	720	90	60		342		144-		144

3.2. СОДЕРЖАНИЕ ОБУЧЕНИЯ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
РАЗДЕЛ 1. Организация и планирование работ по обеспечению защиты предприятия		144	
МДК 01.01 Обеспечение организации систем безопасности предприятия			2
Тема 1.1. Основные понятия безопасности предприятия	Содержание:	0,5	2
	1. Понятие и содержание безопасности предприятия. Цель обеспечения безопасности предприятия.		
	2. Предмет, объекты и субъекты безопасности предприятия		
	Практические занятия:	1	
	1. Концепция безопасности предприятия.		
2. Структура концепции безопасности предприятия. Основные положения.			
Самостоятельная работа обучающихся		4	
Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.			
Тема 1.2. Виды угроз безопасности предприятия	Содержание:	0,5	2
	1. Понятие угроз безопасности предприятия и их		
	2. Сущность и содержание внутренних и внешних угроз безопасности предприятия		
	Практические занятия	1	
	1. Функциональные составляющие обеспечения безопасности предприятия		
Самостоятельная работа обучающихся		4	
Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.			
Тема 1.3. Функциональные	Содержание:	0,5	2

составляющие обеспечения безопасности предприятия	1.	Основные составляющие системы обеспечения безопасности предприятия		
	2.	Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.		
	Практические занятия:		1	
	1.	Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание. Информационная безопасность в системе национальной безопасности РФ		
<i>Самостоятельная работа обучающихся</i>		4		
Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.				
Тема 1.4. Информационная безопасность автоматизированных систем	Содержание:		0,5	2
	1.	Современная постановка задачи защиты информации. Организационно-правовое обеспечение информационной безопасности		
	Практические занятия:		1	
	1.	Информация как объект юридической защиты. Основные принципы засекречивания информации.		
<i>Самостоятельная работа обучающихся</i>		6		
Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.				
Тема 1.5. Информационные системы	Содержание:		0,5	
	1.	Источники конфиденциальной информации в информационных системах.		2
	2.	Виды технических средств информационных систем.		
	Практические занятия:		1	
1.	Общие положения. Информация как продукт. Информационные услуги.			
2.	Неправомерное овладение конфиденциальной информацией в информационных системах.			
<i>Самостоятельная работа обучающихся</i>		6		

	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		
Тема 1.6. Угрозы информации	Содержание:	0,5	2
	1. Классы каналов несанкционированного получения информации. Причины нарушения целостности		
	2. Модель нарушителя информационных систем.		
	Практические занятия:	1	
	1. Виды угроз информационным системам.		
	2. Убытки, связанные с информационным обменом.		
	Самостоятельная работа обучающихся	6	
	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		
Тема 1.7. Методы и модели оценки уязвимости информации	Содержание:	0,5	2
	1. Эмпирический подход к оценке уязвимости информации.		
	Практические занятия:		
	1. Практическая реализация модели «угроза - защита».	1	
		Самостоятельная работа обучающихся	6
	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		
Тема 1.8. Оценки уязвимости информации	Практические занятия:	1	
	1. Рекомендации по использованию моделей оценки уязвимости информации, позволяющих определить текущие и прогнозировать будущие значения всех показателей уязвимости информации для любых компонентов автоматизированной системы обработки данных, любой их комбинации и для любых условий жизнедеятельности		
		Самостоятельная работа обучающихся	6
	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		

Тема 1.9. Методы определения требований к защите информации	Содержание:		1	2
	1.	Требования к защите информации, обусловленные спецификой автоматизированной обработки информации		
	Практические занятия		1	
	1.	Требования, определяемые структурой автоматизированной системы		
Самостоятельная работа обучающихся Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		6		
Тема 1.10. Методики определения требований к защите информации	Содержание:		0,5	2
	1.	Требования к безопасности информационных систем в		
	Практические занятия:		1	
	1.	Требования к безопасности информационных систем в		
	2.	Классы защищенности средств вычислительной техники от несанкционированного доступа.		
	3.	Факторы, влияющие на требуемый уровень защиты информации.	6	
Самостоятельная работа обучающихся Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.				
Тема 1.11 Стратегии защиты информации	Содержание:		0,5	2
	1.	Организация защиты информации.		
	2.	Уровень технологических схем обработки.	1	
	Практические занятия:			
	1.	Уровень структурно-организационного построения объекта обработки информации.		
	2.	Виды стратегии защиты информации.	6	
Самостоятельная работа обучающихся Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.				

Тема 1.12 Архитектура систем защиты информации	Содержание:		0,5	2
	1.	Ресурсы системы защиты информации. Организационное построение.		
	2.	Криптографические методы и средства защиты информации в компьютерных системах и сетях		
	3.	Комплексная защита информации в компьютерных системах и сетях.		
	4.	Безопасность сетевых операционных систем		
	5.	Безопасность локальных и глобальных сетевых технологий		
Самостоятельная работа обучающихся		6		
Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.				
Тема 1.13 Экономическая безопасность предприятия	Содержание:		0,5	2
	1.	Типичная структура экономической безопасности предприятия		
	2.	Трансформация структуры обеспечения экономической безопасности предприятия		
	3.	Уровни экономической безопасности		
	4.	Национальная экономическая безопасность		
	5.	Угрозы экономической безопасности		
	6.	Показатели и индикаторы экономической безопасности предприятия		
	7.	Классификация и оценка экономической безопасности		
	8.	Характеристика состояния экономической безопасности современного предприятия		
	9.	Мониторинг экономической безопасности предприятия. Основные цели мониторинга экономической безопасности предприятия		
Самостоятельная работа обучающихся		6		
Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.				

Тема 1.14 Обеспечение экономической безопасности	Содержание:		0,5	2		
	1.	Функциональные составляющие экономической				
	2.	Корпоративные ресурсы экономической безопасности предприятия				
	3.	Основные подходы к формированию экономической безопасности предприятия				
	4.	Сущность финансовой составляющей экономической безопасности предприятия.				
	5.	Основные индикаторы состояния финансовой составляющей экономической безопасности предприятия.				
	6.	Способы обеспечения финансовой составляющей экономической безопасности предприятия.				
Самостоятельная работа обучающихся		6				
Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.						
Тема 1.15 Отечественные и международные акты обеспечения ИБ	Содержание:		0,5	2		
	1.	Отечественное организационное и нормативно-правовое обеспечение ИБ				
	2.	Международное нормативно-правовое обеспечение ИБ				
	Практические занятия:				4	
	1.	Проведение аудита состояния информационной				
	2.	Определение уязвимостей информационной системы				
	3.	Расчет коэффициентов авторитета экспертов				
Самостоятельная работа обучающихся		6				
Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.						
Тема 1.16 Организационное регулирование защиты процессов переработки информации	Содержание:		0,5	2		
	1.	Категорирование объектов и защиты информационных				
	2.	Ответственность за нарушение законодательства в информационной сфере				
	3.	Анализ и оценка концепций защиты процессов переработки информации				
	Практические занятия:				1	
1.	Построение матрицы парных сравнений уязвимостей					
2.	Составление вектора доступности уязвимостей					

	Самостоятельная работа обучающихся	6	
	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		
Тема 1.17 Организация противодействия технической разведке	Содержание:	0,5	2
	1. Организация противодействия технической разведке. Защита от утечки информации, несанкционированного		
	Практические занятия:	1	
	1. Составление матрицы причинно-следственных связей		
	Самостоятельная работа обучающихся	6	
	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		
Тема 1.18 Программно-аппаратные средства защиты ПЭВМ	Содержание:	0,5	2
	1. Методы и средства ограничения и доступа к компонентам		
	2. Программно-аппаратные средства защиты ЭВМ		
	Практические занятия:	1	
	1. Составление списка элементов информационной системы предприятия		
	2. Составление списка элементов системы защиты		
	Самостоятельная работа обучающихся	6	
	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		
Тема 1.19 Методы и средства обеспечения хранения и переработки ключевой и другой информации	Содержание:	0,5	2
	1. Методы и средства обеспечения хранения и переработки ключевой и другой информации		
	Практические занятия:	1	
	1. Составление перечня количественных и качественных требований к системе защиты информации		
	2. Расчет основных показателей экономической эффективности системы защиты информации		
	Самостоятельная работа обучающихся	6	

	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		
Тема 1.20 Защита программного обеспечения от изучения, вирусного заражения, разрушающих программных действий	Содержание:	0,5	2
	1. Основные классификационные признаки компьютерных вирусов		
	2. Некоторые компьютерные вирусы		
	3. Методы и технологии борьбы с компьютерными вирусами		
	4. Условия безопасной работы компьютерных систем и технология обнаружения заражения вирусами		
	5. Контроль целостности и системные вопросы защиты программ и данных		
	Практические занятия:	1	
	1. Оценка ценности информационных активов предприятия		
	2. Разработка концепции информационной безопасности предприятия		
	<i>Самостоятельная работа обучающихся</i>	6	
Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.			

Темы самостоятельной работы обучающегося

1. Средства и методы обеспечения безопасности предприятия
2. Критерии безопасности предприятия
3. Определение и содержание наиболее важных показателей безопасности предприятия.
4. Основные направления и способы обеспечения безопасности предприятия
5. Построение эффективной системы безопасности предприятия
6. Диагностическое обследование системы безопасности предприятия
7. Последовательность работ при проведении аудита системы безопасности предприятия
8. Государственная информационная политика.
9. Проблемы информационной войны.
10. Проблемы информационной безопасности в сфере государственного и муниципального управления.
11. Государственная система правового обеспечения защиты информации в РФ.
12. Государственная информационная безопасность РФ
13. Законодательство в области информационной безопасности
14. Радиоэлектронные системы и устройства защиты информации

15. Виды потерь.
16. Информационные инфекции.
 17. Система с полным перекрытием.
 18. Политика и модели безопасности
 19. Требования, связанные с размещением защищаемой информации.
 20. Требования, обусловленные видом защищаемой информации.
 21. Анализ существующих методик определения требований к защите информации.
 22. Оценка состояния безопасности ИС. Критерии оценки безопасности информационных технологий.
 23. Методы защиты информации
 24. Средства защиты информации
 25. Требования к криптосистемам. Основные алгоритмы шифрования.
 26. Цифровые подписи. Криптографические хеш-функции.
 27. Криптографические генераторы случайных чисел.
 28. Криптоанализ и атаки на криптосистемы.
 29. Требования к архитектуре СЗИ. Построение СЗИ.
 30. Ядро системы защиты информации.
 31. Управление безопасностью на основе интеграций. Обеспечение безопасности современного предприятия
 32. Использование единого информационного пространства при организации управления безопасностью
 33. Структура единого информационного пространства
 34. Обобщенная архитектура системы управления безопасностью предприятия
 35. Алгоритмы управления безопасностью
 36. Оценка и управление рисками
 37. Управление безопасностью
 38. Алгоритм управление безопасностью
 39. Автоматизированная система управления безопасностью
 40. Модель базы данных системы ИБ предприятия
 41. Метод SRAMM анализа рисков
 42. Программное обеспечение Risk Watch
 43. Модель вероятного нарушителя информационной безопасности
 44. Описание объектов и целей реализации угроз информационной безопасности
 45. Средства защиты денежных средств, материальных ценностей и документации
 46. Проверка лояльности персонала организации
 47. Система кондиционирования воздуха как составная часть безопасности предприятия
48. Системы охранной и пожарной сигнализации

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения	
РАЗДЕЛ 2 Обеспечение организации службы защиты информации		144		
МДК 01.02 Организация работ подразделений защиты информации				
Тема 2.1 Место и роль службы защиты информации в системе защиты информации	Содержание:	1	2	
	1. Назначение службы защиты информации			
	2. Место службы защиты информации в системе безопасности предприятия			
	3. Служба защиты информации как составляющая часть системы защиты информации	2		
	Практические занятия:			
	1 Служба защиты информации как орган управления			
	2 Статус службы защиты информации в структуре безопасности предприятия			
3 Разработка организационно-правовых аспектов деятельности службы защиты информации				
	Самостоятельная работа обучающихся Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.	10	2	
Тема 2.2 Основные задачи и функции службы защиты информации	Содержание:	1	2	
	1. Организационные задачи и функции службы защиты информации			
	2. Технологические задачи и функции службы защиты информации	2		
	Практические занятия:			
	1 Координационные задачи и функции службы защиты информации			
2 Разработка организационной структуры службы защиты информации				
	Самостоятельная работа обучающихся	10	2	

	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		
Тема 2.3 Общая структура и штаты службы защиты информации	Содержание:	1	2
	1. Общая структурная схема службы защиты информации		
	2. Подразделения службы защиты информации		
	3. Факторы, определяющие конкретную структуру службы защиты информации		
	4. Виды и типы организационных структур службы защиты информации		
	5. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ		
	Практические занятия: Задачи, функции, права и ответственность заместителя руководителя предприятия по безопасности в области	2	
	Разработка модели системы защиты информации для службы защиты информации		
	Место и роль службы защиты информации в системе защиты информации		
	Задачи и функции службы защиты информации		
Структура и штаты службы защиты информации			
	<i>Самостоятельная работа обучающихся</i>	10	2
	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		
Тема 2.4 Организационные основы и принципы деятельности службы защиты информации	Содержание:	1	2
	1. Порядок создания службы защиты информации		
	2. Структура и содержание положения о службе защиты информации		
	3. Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации		

	4.	Основные принципы организации и деятельности службы защиты информации		
	1	Практические занятия: Экспертная оценка мероприятий по защите информации в службе защиты информации	2	
	2	Организация труда сотрудников службы защиты информации		
	3	Подбор, расстановка кадров и обучение сотрудников службы защиты информации		
	4	Организационные основы и принципы деятельности службы защиты информации		
	5	Оценка производительности труда по результатам оптимизации процессов в службе защиты информации		
	Самостоятельная работа обучающихся		10	2
	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.			
Тема 2.5 Подбор, расстановка и обучение сотрудников службы защиты информации	Содержание:		1	2
	1.	Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации		
	2.	Особенности подбора кадров		
	3.	Методы получения информации о кандидатурах на должности.		
	4.	Формы повышения квалификации сотрудников. Подготовка кадрового резерва		
	5.	Практические занятия: Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации	2	
	6.	Принципы и методы управления службой защиты информации		
	Самостоятельная работа обучающихся		10	2

	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.			
Тема 2.6	1	Содержание: Состав и характеристика процесса проектирования деятельности службы защиты информации	1	
Технология управления службой защиты информации	1	Практические занятия: Методы организационного проектирования деятельности службы защиты информации	2	
	Самостоятельная работа обучающихся Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		10	2
Тема 2.7 Организация труда сотрудников службы защиты информации	Содержание:		1	2
	1.	Специфика деятельности сотрудников службы защиты информации		
	1	Практические занятия: Распределение обязанностей между сотрудниками службы защиты информации	2	
	Самостоятельная работа обучающихся Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.		12	2
Тема 2.8 Структура и содержание должностных инструкций сотрудников службы защиты информации	3.	Структура и содержание должностных инструкций сотрудников службы защиты информации.	1	
	4.	Практические занятия: Организация рабочих мест сотрудников службы защиты информации	2	
	Самостоятельная работа обучающихся		14	2

	Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.			
Тема 2.9 Принципы и методы управления службой защиты информации	Содержание:	1	2	
	1. Принципы управления службой защиты информации			
	2. Система методов управления.			
	3. Взаимосвязь методов управления			
1	Практические занятия: Необходимость комплексного и системного применения методов управления службой защиты информации.	2		
	Самостоятельная работа обучающихся Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.	14	2	
Тема 2.10 Технология управления службой защиты информации	Содержание:	1	2	
	1. Состав и содержание управленческих функций.			
	1	Практические занятия: Технология управления службой защиты информации.	2	
	2	Значение управленческих решений		
3	Цели планирования			
	Самостоятельная работа обучающихся Конспектирование лекционного материала. Работа с теоретическим материалом лабораторной работы и составление отчета. Подготовка информационных сообщений.	14	2	

Темы самостоятельной работы обучающегося

1. Оптимизация структуры управления службой защиты информации
2. Мероприятия по контролю и мониторингу направлений деятельности службы защиты информации
3. Мероприятия по мониторингу направлений деятельности службы защиты информации
4. Взаимосвязь и соотношение организационных, технологических и координационных задач и функций
5. Факторы, влияющие на определение задач и функций службы защиты информации

6. Централизованная и децентрализованная структуры службы защиты информации, условия, критерии, определяющие выбор структур
7. Факторы, определяющие численность сотрудников службы защиты информации
8. Оценка эффективности работы службы защиты информации
9. Условия и факторы, влияющие на организацию работы службы защиты информации
10. Организация взаимодействия службы защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации
11. Социально-психологические факторы, влияющие на расстановку кадров.
12. Формы создания и способы поддержания необходимого микроклимата в коллективе
13. Обеспечение персональной ответственности за сохранность носителей информации
14. Обеспечение необходимых условий труда.
15. Охрана труда. Культура труда. Карты организации трудового процесса.
16. Понятие и сущность методов управления.
17. Административно-правовые методы управления
18. Экономические методы управления. Социально-психологические методы управления.
19. Виды планирования, их назначение.
20. Содержание и структура планов.
21. Технология планирования.
22. Методы и формы контроля выполнения планов
23. Критерии эффективности службы защиты информации.
24. Пути и способы повышения эффективности управления службой защиты информации. Мероприятия по мониторингу направлений деятельности службы защиты информации

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
РАЗДЕЛ 3. Особенности организации работ с конфиденциальными документами		144	
МДК 01.03. Организация работы персонала с конфиденциальной информацией			
Тема 3.1 Понятие о конфиденциальных документах	Содержание:	1	2
	1. Общие положения. Классификация информации и документов по категориям доступа		
	2. Понятие ценной и конфиденциальной информации. Перечень сведений конфиденциального характера		
	3. Представление и распространение информации. Персональные данные		
	4. Тайна следствия и судопроизводства. Служебная тайна. Профессиональная тайна. Коммерческая тайна. Ноу-хау.		
	5. Нормативная база конфиденциального делопроизводства.	2	
	Практические занятия:		
1. Обработка персональных данных без использования средств информатизации.			
	2. Нормативно-правовая база организации работы с конфиденциальными документами.		
Тема 3.2 Особенности работы с конфиденциальной информацией	Содержание:	1	2
	1. Особенности документирование конфиденциальной информации		
	2. Оформление реквизитов конфиденциальных документов при документировании информации		
	3. Ограничение доступа к документам и использование отметки конфиденциальности при оформлении документов		
	4. Перечень конфиденциальной информации		
	5. Основные этапы разработки перечня конфиденциальной документированной информации		
6. Учет бумажных носителей информации и их проектов			

	Практические занятия:	2	
	1. Разработка перечня документированной конфиденциальной информации		
	2. Определение степени разграничения доступа к документам и использование отметки конфиденциальности при оформлении документов		
Тема 3.3 Особенности организации конфиденциального документооборота	Содержание:	1	2
	1. Учет и регистрация конфиденциальной документированной информации		
	2. Обработка поступающих конфиденциальных документов, их учет и регистрация		
	3. Технология исполнения и контроля за исполнением конфиденциальных документов		
	4. Учет и регистрация внутренних, исходящих и внешних конфиденциальных документов		
	5. Учет конфиденциальной документированной информации выделенного хранения		
	Практические занятия:	2	
	1. Обработка поступающих и внутренних конфиденциальных документов, их учет и регистрация		
	2. Учет и регистрация внутренних конфиденциальных документов		
		3. Исполнение и контроль за исполнением конфиденциальных документов	
Тема 3.4 Текущая работа с персоналом, обладающим конфиденциальной информацией	Содержание:	1	2
	1. Профессиональная ориентация и обучение персонала		
	2. Мотивация персонала к выполнению требований по защите информации.		
	Практические занятия:	2	
	1. Подбор персонала на должности, связанные с работой с конфиденциальной информацией.		
	2. Допуск к секретной информации.		
	3. Организация работы с персоналом, имеющим доступ к конфиденциальной информацией.		

Тема 3.5 Охрана территории, зданий, помещений и персонала	Содержание:		2	2
	1.	Понятие "охрана". Цели и задачи охраны.		
	Практические занятия:		4	
	1.	Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия		
2.	Порядок назначения комиссии для аттестации помещений на пригодность их для ведения конфиденциальных работ			
	3.	Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных изделий и документов		
Тема 3.6 Организация пропускного и внутри объектового режимов	Содержание:		2	2
	1.	Понятие "пропускной режим". Цели и задачи пропускного режима. <i>Особенности охраны персонала</i>		
	2.	Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков		
	Практические занятия:		4	
	1.	Организация подготовки и проведения совещаний и переговоров		
	2.	Организация защиты информации при приеме в организации посетителей и командированных лиц.		
	3.	Организация защиты информации при приеме в организации иностранных представителей.		
Тема 3.7 Подготовка и	Содержание:		2	2

проведение совещаний и переговоров по конфиденциальным вопросам	1.	Основные требования, предъявляемые к подготовке и проведению совещаний и переговоров по конфиденциальным вопросам. Порядок назначения ответственных лиц и их обязанности по проведению совещаний и переговоров	4	2
	Практические занятия:			
	1.	Организация защиты информации при осуществлении рекламной и публикаторской деятельности.		
	2.	Организация защиты информации при подготовке материалов к открытому опубликованию		
	3.	Аналитическая работа как основа управления системой организационной защиты информации		
	4.	Планирование процессов организационной защиты информации		
	5.	Контроль функционирования системы организационной защиты информации		
Самостоятельная работа обучающегося			114	3
1. Законы РФ «О коммерческой тайне», «Об информации, информатизации и защите информации», «О персональных данных» 2. Нормативно-методическая база организации работы с документами, содержащими служебную тайну 3. Сущность и принципы ограничения доступа к информации и документам 4. Нормативно-правовые основы организации работы с документами, содержащими коммерческую тайну 5. Создание и изготовление конфиденциальных документов с помощью ЭВМ их печатания, тиражирования и размножения. 6. Учет использования и хранения печатей, штампов, бланков, необходимых для оформления документов 7. Понятие "внутри объектовой режим". Его основное назначение при ведении конфиденциальных работ и обращении с охраняемыми изделиями и документами				

8. Порядок определения перечня предметов, запрещенных к проносу провозу на режимную территорию. Общие требования внутри объектового режима.
9. Экспедиционные технологии обработки и учета поступающих пакетов с конфиденциальной информацией
10. Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта.
11. Порядок допуска работников в помещения, где ведутся конфиденциальные работы.
12. Организация работы по защите информации при осуществлении публицистической деятельности и связей с прессой; участие в ней Службы безопасности
13. Организация контроля за выполнением распорядка дня лицами, работающими на режимных объектах.
14. Создание отдельных (выделенных) производственных зон (зон доступа) по типу и степени конфиденциальности работ с самостоятельными системами организации и контроля доступа.
15. Методика проектирования системы пропускного и внутри объектового режимов и оценки эффективности их функционирования.
16. Организация работы по защите информации при осуществлении публицистической деятельности и связей с прессой; участие в ней
17. Службы безопасности
18. Методы оценки эффективности защитных мероприятий в рекламной и публицистической деятельности.
19. Виды и способы охраны. Понятие о рубежах охраны. Много рубежная система охраны
20. Много рубежная система охраны
21. Порядок вывоза (выноса) материальных ценностей и документации с территории организации и ввоза (вноса) их на территорию
22. Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта. Порядок допуска работников в помещения, где ведутся конфиденциальные работы
23. Методика проектирования системы пропускного и внутри объектового режимов и оценки эффективности их функционирования

<p>24. Составление списков участников совещания 25. Определение состава информации, используемой в ходе совещаний, переговоров</p>		
<p>Учебная практика (по профилю специальности) Виды работ Разработка должностной инструкции охранника объекта Разработка должностной инструкции начальника охраны объекта Подготовка проекта установки камер внешнего видеонаблюдения объекта Подготовка проекта установки камер внутреннего видеонаблюдения объекта Составление технического регламента работы с конфиденциальной информацией для персонала, имеющего допуск к конфиденциальной информации Составление технического регламента о порядке оформления допуска лиц к конфиденциальным сведениям Составление технического регламента работы с системой внешнего видеонаблюдения Составление технического регламента работы с системой внутреннего видеонаблюдения Составление технического регламента организации и проведения рабочих совещаний</p>	<p>114</p>	<p>3</p>
<p>Производственная практика (по профилю специальности) Виды работ Подготовка проекта выделения зон доступа по типу работ на объекте. Подготовка проекта выделения зон доступа по конфиденциальности работ объекте Подготовка проекта установки СКУД на объекте</p>	<p>114</p>	<p>3</p>

<p>Составление технического регламента работы с СКУД объекта Составление Положения об охране персонала объекта Составление Положения о режимных помещениях объекта Подготовка проекта оборудования режимного помещения объекта Составление технического регламента организации и проведения совещаний по конфиденциальным вопросам Составление Положения о подразделении защиты информации Составление Положения о проверке персонала по защите информации Составление Положения о защите информации при приеме посетителей на объекте Составление Положения о процедуре служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией Составление Положения об организации работы при осуществлении международного сотрудничества Составление технического регламента контроля соблюдения персоналом требований режима защиты информации на объекте Проведение исследования о целесообразности внедрения биометрических систем безопасности на объекте Проведение технического аудита системы видеонаблюдения объекта Проведение технического аудита СКУД объекта Проведение технического аудита безопасности компьютерных систем объекта Составление технического регламента работы с компьютерными системами объекта Составление технического регламента защиты информации в процессе рекламной деятельности Проведение технического аудита организации охраны объекта Проведение исследования о соответствии подбора и расстановки сотрудников</p>	
Всего	720

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (узнавание ранее изученных объектов, свойств);

2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. ТРЕБОВАНИЯ К МИНИМАЛЬНОМУ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ

Реализация профессионального модуля предполагает наличие учебного кабинета «Информационной безопасности»; лабораторий «Электронного документооборота» и «Технических средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя;
- рабочие места по количеству обучающихся;
- комплекты учебно-методической документации;
- наглядные пособия;

Технические средства обучения:

- мультимедийный проектор;
- интерактивная доска;
- компьютеры;
- многофункциональные устройства

4.2 ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОБУЧЕНИЯ

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

Основные источники:

1. Шаньгин П.П. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: Издательство «Форум», 2013.-416 с. Рекомендовано МО РФ.

Дополнительные источники:

1. Ефремов, И. Информационные технологии в сфере безопасности: практикум: И. Ефремов, В. Солопова; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - Оренбург: ОГУ, 2013. - 116 с. <http://biblioclub.ru/index.php?page=book&id=259178>
2. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов. - М.: Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. <http://biblioclub.ru/index.php?page=book&id=362895>
3. Некраха, А.В. Организация конфиденциального делопроизводства и защита информации: учебное пособие / А.В. Некраха, Г.А. Шевцова; Институт информационных наук и технологий безопасности, Российский государственный

гуманитарный университет. - М.: Академический проект, 2012. - 222 с.
Рекомендовано УМО <http://biblioclub.ru/index.php?page=book&id=143604>

4. Нестеров, С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб: Издательство Политехнического университета, 2014. - 322 с.: схем, табл., ил. <http://biblioclub.ru/index.php?page=book&id=363040>
5. Организация безопасной работы информационных систем: учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др.; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с.: ил. <http://biblioclub.ru/index.php?page=book&id=277794>

Интернет-ресурсы:

1. <http://www.management.com.ua/ims/ims031.html>
2. <http://www.intuit.ru/department/se/devis/>
3. http://www.interface.ru/fset.asp?Url=/case/proekt_inf_sis2.htm
4. <http://www.s-networks.ru/index-194.shtml.htm>
5. <http://www.npp-bit.ru>
6. <http://infosec2006.ucoz.ru>

4.3. ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Профессиональный модуль ПМ.01 «Участие в планировании и организации работ по обеспечению защиты объекта» входит в состав профессионального цикла. Дисциплины, изучение которых должно предшествовать освоению данного модуля: Учебные дисциплины:

- Документоведение
- Документационное обеспечение управления
- Архивоведение
- Технические средства информатизации
- Базы данных
- Основы информационной безопасности
- Экономика организации
- Организационные основы деятельности организации
- Менеджмент
- Безопасность жизнедеятельности
- Основы электротехники
- Основы электроники и цифровой схемотехники
- Средства обработки и хранения информации
- Охрана труда и техника безопасности
- Web-технологии
- Компьютерные сети

- Криптографические методы защиты информации
- Мультимедийные технологии
- Физические основы защиты информации

При освоении профессионального модуля предусматривается использование в образовательном процессе активных и интерактивных форм проведения занятий с применением электронных образовательных ресурсов, деловых игр, индивидуальных и групповых проектов, анализа производственных ситуаций, психологических и иных тренингов, групповых дискуссий в сочетании с внеаудиторной работой для формирования и развития общих и профессиональных компетенций обучающихся.

Текущий контроль проводится в форме: устного опроса, защиты практических работ по МДК.01.01, МДК.01.03, выполнение и защита курсовой работы по МДК.01.01. Предусматривается сдача зачётов МДК.01.01., МДК.01.02, МДК.01.03 и экзамена по МДК.01.01.

Реализация программы модуля предполагает обязательную учебную и производственную практику, которая проводится в конце профессионального модуля.

При реализации программы ПМ «Участие в планирование и организации работ по обеспечению защиты объекта» предусматривается учебная и производственная практика (по профилю специальности). Практика является обязательным разделом ОПОП. Она обеспечивает практико-ориентированную подготовку обучающихся.

Учебная практика проводится в лабораториях института и направлена на отработку практических навыков, обеспечивающих освоение профессиональных компетенций, предусмотренных программой профессионального модуля.

Производственная практика (по профилю специальности) проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся.

Аттестация по итогам производственной практики проводится с учетом (или на основании) результатов, подтвержденных документами соответствующих организаций.

Производственная практика (по профилю специальности) завершается зачётом.

Освоение междисциплинарного курса заканчивается экзаменом, освоение программы профессионального модуля - проведением экзамена (квалификационного).

4.4. КАДРОВОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу: наличие высшего профессионального образования, соответствующего профилю модуля «Участие в планировании и организации работ по обеспечению защиты объекта» по специальности 090905 «Организация и технология защиты информации».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: реализация программы профессионального модуля ПМ.01 «Участие в планировании и организации работ по обеспечению защиты объекта» должна обеспечиваться дипломированными специалистами - преподавателями междисциплинарных курсов с обязательной стажировкой в профильных организациях не реже 1-го раза в 3 года.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Целями освоения дисциплины является формирование у студентов чёткого представления о планировании и организации работ по обеспечению защиты объекта.

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.	<ul style="list-style-type: none"> - определение методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации; - выполнение анализа научной литературы; - обоснование выбора соответствующих решений по защите информации объекта; - обоснование использованных методов обнаружения технических каналов утечки информации 	<p>Текущий контроль:</p> <ul style="list-style-type: none"> - ситуационные задачи, - практические работы, работа, - защита работ на различных этапах производственной практики.
ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте	<ul style="list-style-type: none"> - определение предложений по разработке программ защиты информации на объекте; - определение методик защиты информации на предприятии 	<p>Текущий контроль:</p> <ul style="list-style-type: none"> - опрос, - практические работы, работа, - защита работ на различных этапах производственной практики.
ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации	<ul style="list-style-type: none"> - выполнение работ по защите конфиденциальной информацией; - определение качества защиты информации; - выполнение мероприятий по комплексной защите информации 	<p>Текущий контроль:</p> <ul style="list-style-type: none"> - ситуационные задачи, - опрос, - практические работы, работа, - защита работ на различных этапах производственной практики.
ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной	<ul style="list-style-type: none"> - обоснование выбранных организационных решений на объектах информатизации; - обоснование мер по внедрению организационных решений предприятия; 	<p>Текущий контроль:</p> <ul style="list-style-type: none"> - ситуационные задачи, - опрос, - практические работы, работа,

деятельности		- защита работ на различных этапах производственной практики.
ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации	обоснование использования носителей конфиденциальной информации; - определение методики обработки и хранения защищаемой информации; - организация выполнения передачи конфиденциальной информации на различных носителях. - полнота и эффективность соблюдения правил использования носителей секретной информации	Текущий контроль: - ситуационные задачи, - опрос, - практические работы, работа, - защит работ на различных этапах производственной практики.
ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий	определение правил техники безопасности при комплексной защите информации; - определение методики защиты информации при проведении организационно-технических мероприятий.	Текущий контроль: - ситуационные задачи, - опрос, - практические работы, работа, защит работ различных этапах производственной практики.
ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите	- обоснование выбранных методов проверок организаций, информация которых подлежит защите; - проведение проверки объектов информатизации; - проведение проверки организаций, работающих с конфиденциальной информацией.	Текущий контроль: - ситуационные задачи, - опрос, - практические работы, работа, защит работ различных этапах производственной практики.
ПК 1.8. Проводить контроль за соблюдением персоналом требований режима защиты информации	- определение методов и способов контроля персонала, работающего с конфиденциальной информацией; - определение последовательности действий при проведении проверок соблюдения персоналом требований режима защиты информации; - организация проведения контроля за работой персонала, задействованного в защите информации организации.	Текущий контроль: - ситуационные задачи, - опрос, - практические работы, работа, защит работ различных этапах производственной практики.
ПК 1.9. Участвовать в оценке качества защиты объекта	- выполнение оценки качества комплексной защиты информации организации; - выполнение оценки качества защиты объекта информатизации; - определение и анализ недостатков качества защиты информации на	Текущий контроль: - ситуационные задачи, - опрос, - практические работы, работа, защит работ

	предприятии.	различных этапах производственной практики.
--	--------------	---

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.

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	<ul style="list-style-type: none"> - демонстрация понимания целей и задач профессиональной деятельности; - осознание способов деятельности, выбор средств, адекватных ее целям и задачам 	<ul style="list-style-type: none"> - опрос, - практические работы, - самостоятельная работа, - защита работ на различных этапах производственной практики
ОК 2. Организовывать свою собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	<ul style="list-style-type: none"> - выбор и применение методов и способов решения профессиональных задач в организации и технологии защиты информации; - оценка эффективности и качества выполнения работ. 	
ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	<ul style="list-style-type: none"> - рациональность решения стандартных профессиональных задач в области защиты информации; - аргументированность самоанализа выполнения профессиональных задач 	
ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития	<ul style="list-style-type: none"> - эффективный поиск необходимой информации; - использование различных источников, включая электронные 	
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности	<ul style="list-style-type: none"> - использование программ автоматизации профессиональной деятельности (владеть навыками работы в специальных программах, а также текстовых и табличных редакторах, программах по созданию презентаций). 	

ОК 6. Работать в коллективе и команде, обеспечивать её сплочение, эффективно общаться с коллегами, руководством, потребителями	- взаимодействие с обучающимися, преподавателями, мастерами, руководителями практик от предприятия в ходе обучения	
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий	- самоанализ и коррекция результатов собственной работы при выполнении практических заданий в группе, при подготовке к внеклассным мероприятиям	
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	- организация самостоятельных занятий при изучении профессионального модуля	
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности	- анализ инноваций в области защиты информации	
ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)	- демонстрация готовности к исполнению воинской обязанности	
ОК 11. Применять математический аппарат для решения различных задач.	- уметь применять средства математической логики для решения задач	
ОК 12. Оценивать значимость документов, применяемых в профессиональной деятельности	уметь оценивать документы, используемые в области защиты информации.	
ОК 13. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность	- владение информацией о структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность	