ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ

«ДМИТРОВСКИЙ ТЕХНИКУМ»

ОДОБРЕНО
на заседании ПЦК
_____
«28» августа 2020г.
Протокол № 6

УТВЕРЖДАЮ
Зам. директора по учебно-методической работе
ГБПОУ МО «Дмитровский техникум»
_____ /Н.Е.Горюшкина /
«28» 08 2020г.

РАБОЧАЯ ПРОГРАММА

Профессионального модуля ПМ.01. «Участие в планировании и организации работ по обеспечению защиты объекта»

специальность 10.02.01 Организация и технология защиты информации

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Московской области «Дмитровский техникум

СОГЛАСОВАНО
_____
_____ Н. Н. Гостева
«_28_»_____08_____2020 г.

Александровская И.Л.
2021.04.30 10:04:
31+03'00'

Дмитров, 2020г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования 10.02.01 «Организация и технология защиты информации».

Организация-разработчик: ГБПОУ МО «Дмитровский техникум»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы по подготовке специалистов среднего звена в соответствии с ФГОС СПО по специальности **10.02.01 Организация и технология защиты информации**, входящей в укрупненную группу специальностей **100000 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 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

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 -492 час, включая:
обязательной аудиторной учебной нагрузки обучающегося - 328 часа;
самостоятельной работы обучающегося - 164 часов;
учебная практика – 36 часов;
производственная практика по профилю специальности - 108 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности **Применение программно-аппаратных**

и технических средства защиты информации, в том числе профессиональными и общими 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
ОК 1	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.
ОК 3	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, 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. Объем профессионального модуля и виды учебной работы
ПМ.01Участие в планировании и организации работ по обеспечению защиты объекта

Коды профессиональных компетенций	**Наименования разделов профессионального модуля**	**Всего,** часов	**Объём времени, отведённый на освоение междисциплинарного курса (курсов)**			**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося		**Самостоятельная работа обучающегося,** часов	**Учебная,** часов	**Производственная (по профилю специальности),** часов
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
ПК 1.1. ПК 1.2 ПК 1.3. ПК 1.4.	**МДК 01.01** Обеспечение организации систем безопасности предприятия	**186**	**134**	**64**	**67**		
ПК 1.6. ПК 1.7.	**МДК 01.02** Организация работ подразделений защиты информации	**150**	**100**	56	**50**		
ПК 1.5. ПК 1.8. ПК 1.9.	**МДК 01.03.** Организация работы персонала с конфиденциальной информацией	**150**	**100**	**60**	**50**		
ПК 1.1- ПК 1.9	Учебная практика	**36**	**36**			**36**	
ПК 1.1- ПК 1.9	Производственная практика (по профилю специальности), часов	**108**	**108**				**108**
	Всего	**636**	**472**	**180**	**167**	**36**	**108**

3.2. Содержание обучения по профессиональному модулю

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

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объём часов	Уровень освоения
1	**2**	**3**	**4**
МДК 01.01 Обеспечение организации систем безопасности предприятия		**186**	
РАЗДЕЛ 1. Общие положения безопасности предприятия		**26**	
Тема 1.1. Создание службы безопасности предприятия	**Содержание**	**8**	
	Причины и цели создания службы безопасности предприятия Виды угроз безопасности предприятия Объект безопасности предприятия Задачи службы безопасности предприятия Принципы функционирования службы безопасности предприятия	4	**2**
	Самостоятельная работа обучающегося Средства и методы обеспечения безопасности предприятия Критерии безопасности предприятия	4	

	Определение и содержание наиболее важных показателей безопасности предприятия		
Тема 1.2. Основные подсистемы службы безопасности предприятия	**Содержание**	**10**	
	Экономическая безопасность Техногенная безопасность Экологическая безопасность Информационная безопасность Психологическая безопасность Пожарная безопасность	4	**2**
	Самостоятельная работа обучающегося Определение и содержание наиболее важных показателей безопасности предприятия. Основные направления и способы обеспечения безопасности предприятия	6	
Тема 1.3. Политика и стратегия безопасности	**Содержание**	**8**	
	Показатели критерия эффективности работы службы безопасности Общие ориентиры политики безопасности предприятия Типы стратегий безопасности Средства обеспечения безопасности Концепция безопасности предприятия	4	**2**

	Цели обеспечения безопасности предприятия Субъекты безопасности предприятия Методы обеспечения безопасности		
	Самостоятельная работа обучающегося Построение эффективной системы безопасности предприятия	4	
РАЗДЕЛ 2. Структура и функции службы безопасности предприятия		**28**	
Тема 2.1. Структура службы безопасности предприятия	**Содержание**	**10**	
	Отдел физической охраны и режима Отдел безопасностивнешней деятельности Отдел внутренней безопасности. Отдел защиты информации Отдел психологической безопасности Составление модели службы безопасности коммерческого предприятия	4	**2**
	Самостоятельная работа обучающегося Проверка лояльности персонала организации Система кондиционирования воздуха как составная часть безопасности предприятия Системы охранной и пожарной сигнализации	6	

Тема 2.2. Основные функции службы безопасности предприятия	**Содержание**	**14**	
	Установление обстоятельств недобросовестной конкуренции со стороны других предприятий Сбор информации о лицах, заключивших с предприятием контракты Выявление некредитоспособных партнеров Выявление ненадежных деловых партнеров Сбор сведений по гражданским делам Сбор информации для проведения деловых переговоров Защита жизни и здоровья персонала от противоправных посягательств Защита жизни и здоровья руководства от противоправных посягательств Охрана имущества предприятия Составить схему видов недобросовестной конкуренции Сбор сведений по уголовным делам Расследование фактов разглашения коммерческой тайны предприятия Содержание информации о личности проверяемого Расследование фактов неправомерного использования товарных (фирменных) знаков предприятия Розыск без вести пропавших сотрудников Характеристика действий некредитоспособного партнера Факторы, определяющие ненадежность делового партнера	10	**2**

	Определение случаев необходимости сбора информации Изучение негативных аспектов рынка Действия службы безопасности на всех этапах переговоров Классификация имущества по важности охраны		
	Самостоятельная работа обучающегося Средства защиты денежных средств, материальных ценностей и документации. Проверка лояльности персонала организации. Алгоритмы управления безопасностью	4	
Тема 2.3. Способы и формы участия сотрудников в обеспечении безопасности предприятия	**Содержание**	**4**	
	Значение человеческого фактора приобеспечении безопасности предприятия Группы организационных мероприятий по работе с персоналом Сложности в работе с персоналом	2	**2**
	Самостоятельная работа обучающегося Проверка лояльности персонала организации	2	
РАЗДЕЛ 3. Экономическая и информационная безопасность предприятия		**51**	
Тема 3.1 Экономическая безопасность предприятия	**Содержание**	**12**	
	Национальная экономическая безопасность Уровни экономической безопасности Типичная структура экономической безопасности предприятия	6	**2**

	Трансформация структуры обеспечения экономической безопасности предприятия Угрозы экономической безопасности Показатели и индикаторы экономической безопасности предприятия Классификация и оценка экономической безопасности Характеристика состояния экономической безопасности современного предприятия Мониторинг экономической безопасности предприятия. Основные цели мониторинга экономической безопасности предприятия		
	Самостоятельная работа обучающегося Государственная информационная политика. Проблемы информационной войны. Проблемы информационной безопасности в сфере государственного и муниципального управления. Государственная система правового обеспечения защиты информации в РФ. Государственная информационная безопасность РФ Законодательство в области информационной безопасности	6	
Тема 3.2 Обеспечение	**Содержание**	**10**	

экономической безопасностипредприятия	Функциональные составляющие экономической безопасности Корпоративные ресурсы экономической безопасности предприятия Основные подходы к формированию экономической безопасности предприятия Сущность финансовой составляющей экономической безопасности предприятия. Основные индикаторы состояния финансовой составляющей экономической безопасности предприятия. Способы обеспечения финансовой составляющей экономической безопасности предприятия.	4	
	Самостоятельная работа обучающегося Управление безопасностью на основе интеграций. Обеспечение безопасности современного предприятия Структура единого информационного пространства Обобщенная архитектура системы управления безопасностью предприятия Алгоритмы управления безопасностью Оценка и управление рисками Управление безопасностью Алгоритм управление безопасностью Автоматизированная система управления безопасностью	6	**2**
Тема 3.3Обеспечение	**Содержание**	**32**	

информационной безопасности предприятия	Современная постановка задачи защиты информации. Организационно-правовое обеспечение информационной безопасности. Основные принципы засекречивания информации. Источники конфиденциальной информации в информационных системах Виды технических средств информационных систем Неправомерное овладение конфиденциальной информацией в информационных системах. Виды угроз информационным системам Убытки, связанные с информационным обменом Практическая реализация модели «угроза - защита». Требования к безопасности информационных систем в России Требования к безопасности информационных систем в США Классы защищенности средств вычислительной техники от несанкционированного доступа. Факторы, влияющие на требуемый уровень защиты информации. Классы задач защиты информации Уровень структурно-организационного построения объекта обработки информации Виды стратегии защиты информации Комплексная защита информации в компьютерных системах и сетях. Безопасность сетевых операционных систем	10	**2**

	Безопасность локальных и глобальных сетевых технологий Отечественное организационное и нормативно-правовое обеспечение ИБ Международное нормативно-правовое обеспечение ИБ Ответственность за нарушение законодательства в информационной сфере Защита от утечки информации, несанкционированного доступа Методы и средства ограничения и доступа к компонентам ЭВМ Программно-аппаратные средства защиты ЭВМ	
	Самостоятельная работа обучающегося Законодательство в области информационной безопасности Радиоэлектронные системы и устройства защиты информации Виды потерь. Информационные инфекции. Требования, связанные с размещением защищаемой информации. Требования, обусловленные видом защищаемой информации. Анализ существующих методик определения требований к защите информации. Оценка состояния безопасности ИС. Критерии оценки безопасности информационных технологий. Методы защиты информации Средства защиты информации Требования к криптосистемам. Основные алгоритмы шифрования.	**22**

	Управление безопасностью на основе интеграций. Обеспечение безопасности современного предприятия Структура единого информационного пространства	
Курсовой проект Тема курсовой работы: Подготовка объектов информатизации предприятия к аттестации по требованиям защиты конфиденциальной информации» (объекты согласно утвержденного перечня).		**20**
Практические занятия Общие понятия обеспечения безопасности информации Цели, задачи и принципы построения КСЗИ Система охраны, пропускного и внутри объектового режима Разработка политики безопасности и регламента безопасности организации Требования к КСЗИ Изучение этапов разработки КСЗИ Организация работы с персоналом предприятия Конструктивные особенности организации, как фактор, влияющий на КСЗИ Задачи, влияющие на определение состава защищаемой информации Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия Изучение методики выявления состава носителей защищаемой информации		**58**

Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа Угрозы безопасности информации Модели нарушителей безопасности АС Технические каналы утечки информации Перехват информации по радиоканалу при использовании специальных технических средств Вероятность обнаружения и распознавания объектов наблюдения по оптическому каналу Средства видеонаблюдения и их установка Методы и способы защиты данных. Классификация СЗИ от НСД Механизмы обеспечения безопасности информации Оптимальное построение системы защиты для автоматизированной системы Определение основных условий функционирования КСЗИ Основные угрозы безопасности информации АС организации Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов Анализ мероприятий по ЗИ объекта Разработка системы контроля вскрытия аппаратуры (СКВА) для заданного объекта Построение модели объекта защиты Модель возможного нарушителя и угроз безопасности Меры по защите информации в рамках построения КСЗИ Особенности защиты информации в кабинете руководителя предприятия	

Анализ и использование результатов проведения контрольных мероприятий в области защиты информации Практические действий работников при чрезвычайных ситуациях Определение требований к средствам вычислительной техники (СВТ). Определение требований к автоматизированным системам (АС). Методы проведения экспертного опроса Определение затрат на защиту информации.			
МДК 01.02 Организация работ подразделений защиты информации		**156**	
РАЗДЕЛ 1. Обеспечение организации службы защиты информации		**44**	
Тема 1.1. Место и роль службы защиты информации в системе защиты информации	**Содержание**	**16**	
	Назначение службы защиты информации Место службы защиты информации в системе безопасности предприятия Служба защиты информации как составляющая часть системы защиты информации Служба защиты информации как орган управления защитой информации Статус службы защиты информации в структуре безопасности предприятия Разработка организационно-правовых аспектов деятельности службы защиты информации	8	**2**

Тема 1.2. Основные задачи и функции службы защиты информации	**Содержание** Организационные задачи и функции службы зашиты информации Технологические задачи и функции службы защиты информации Координационные задачи и функции службы защиты информации Разработка организационной структуры службы защиты информации	8	**2**
Тема 1.3. Общая структура и штаты службы защиты информации	**Содержание**	**8**	
	Общая структурная схема службы защиты информации Подразделения службы защиты информации Факторы, определяющие конкретную структуру службы защиты информации Виды и типы организационных структур службы защиты информации Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ Задачи, функции, права и ответственность заместителя руководителя предприятия по безопасности в области защиты информации Разработка модели системы защиты информации для службы защиты информации Место и роль службы защиты информации в системе защиты информации	8	**2**

	Задачи и функции службы защиты информации Структура и штаты службы защиты информации		
Тема 1.4. Организационные основы и принципы деятельности службы защиты информации	**Содержание**	**8**	
	Порядок создания службы защиты информации Структура и содержание положения о службе защиты информации Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации Основные принципы организации и деятельности службы защиты информации Экспертная оценка мероприятий по защите информации в службе защиты информации Организация труда сотрудников службы защиты информации Подбор, расстановка кадров и обучение сотрудников службы защиты информации Организационные основы и принципы деятельности службы защиты информации Оценка производительности труда по результатам оптимизации процессов в службе защиты информации	8	2
Тема 1.5. Организация	**Содержание**	**4**	

труда сотрудников службы защиты информации	Специфика деятельности сотрудников службы защиты информации Распределение обязанностей между сотрудниками службы защиты информации Структура и содержание должностных инструкций сотрудников службы защиты информации. Организация рабочих мест сотрудников службы зашиты информации Принципы управления службой защиты информации	4	**2**
Тема 1.6. Подбор, расстановка и обучение сотрудников службы защиты информации	**Содержание**	**6**	
	Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации Особенности подбора кадров Методы получения информации о кандидатурах на должности. Формы повышения квалификации сотрудников. Подготовка кадрового резерва Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации Принципы и методы управления службой защиты информации Технология управления службой защиты информации Состав и характеристика процесса проектирования деятельности службы защиты информации Методы организационного проектирования деятельности службы защиты информации	6	2
Тема 1.7. Технология управления службой	**Содержание**	**2**	
	Состав и содержание управленческих функций.	2	

защиты информации	Технология управления службой защиты информации. Значение управленческих решений Цели планирования		**2**
Практические занятия Служба защиты информации как координатор деятельности по обеспечению безопасности информации Факторы, влияющие на определение задач и функций службы защиты информации. Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений защиты информации. Факторы, определяющие численность сотрудников подразделений защиты информации. Порядок взаимодействия подразделений защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации Организация взаимодействия службы защиты информации и подразделений предприятия Особенности подбора кадров. Методы получения информации о кандидатурах на должности. Социально-психологические факторы, влияющие на расстановку кадров. Обеспечение персональной ответственности за сохранность носителей информации. Специфика деятельности сотрудников службы защиты информации Распределение обязанностей между сотрудниками подразделений защиты информации. Проектирование структуры службы защиты информации Организационные основы и принципы деятельности службы защиты информации. Пакет документов. Система конфиденциальной информации фирмы Организация информационно-аналитической работы. Методы оценки качества подразделений защиты информации. Пути повышения эффективности управления подразделениями защиты информации. Методы оценки качества службы защиты информации. Методика определения численного состава подразделений защиты информации.		**56**	**2,3**
Самостоятельная работа обучающегося 1. Оптимизация структуры управления службой защиты информации		**50**	**3**

2. Мероприятия по контроля 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			
МДК 01.03. Организация работы персонала с конфиденциальной информацией		**150**	
РАЗДЕЛ 1. Особенности организации работ с конфиденциальными документами		**40**	
Тема1.1. Конфиденциальные сведения	**Содержание**	**2**	
	Перечень сведений конфиденциального характера	2	**2**
Тема1.2. Коммерческая тайна	**Содержание**	**6**	
	Понятие коммерческой тайны. Принципы отнесения информации к коммерческой тайне Условия обеспечения сохранности конфиденциальных документов Сведения, относящиеся к коммерческой тайне Сведения, не относящиеся к коммерческой тайне	6	**2**
Тема1.3. Организация	**Содержание**	**4**	

работы с документами, содержащими конфиденциальные сведения	Основная цель защиты конфиденциальной информации Меры по охране конфиденциальности информации	4	**2**
Тема1.4. Защита документов, содержащих коммерческую тайну	**Содержание**	**16**	
	Памятка о сохранении коммерческой тайны предприятия Ведение конфиденциального делопроизводства Учет документов, содержащих конфиденциальные сведения Ограничения при работе с конфиденциальными документами Ежегодный контроль конфиденциальных документов Действия при утере конфиденциальных документов Передача конфиденциальных документов при увольнении сотрудника Сдача конфиденциальных документов в архив	16	**2**
Тема1.5. Уничтожение документов	**Содержание**	**2**	
	Правила уничтожения документов	2	**2**
Тема1.6. Текущая работа с персоналом, обладающим конфиденциальной информацией	**Содержание**	**2**	
	Профессиональная ориентация и обучение персонала Мотивация персонала к выполнению требований по защите информации.	2	**2**
Тема1.7. Охрана	**Содержание**	**2**	

территории, зданий, помещений и персонала	Понятие "охрана". Цели и задачи охраны. Виды и способы охраны объекта.	2	**2**
Тема1.8. Подготовка и проведение совещаний и переговоров по конфиденциальным вопросам	**Содержание**	**6**	
	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	6	**2**
Практические занятия Классификация документов по грифу ограничения доступа Научно-техническая (технологическая) информация,относящаяся к коммерческой тайне Деловая информация, относящаяся к коммерческой тайне Комплекс мер по обеспечению защиты конфиденциальной информации Допуск работника к конфиденциальной информации Обязательство о неразглашении коммерческой тайны Грифы ограничения доступа Журнал регистрации документов с грифом "Коммерческая тайна" Журнал учета выдачи документов с грифом "Коммерческая тайна" Степени секретности служебных документов Виды уничтожителей конфиденциальных документов Подбор персонала на должности, связанные с работой с конфиденциальной информацией.		**60**	**2**

Допуск к секретной информации. Организация работы с персоналом, имеющим доступ к конфиденциальной информации. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия Порядок назначения комиссии для аттестации помещений на пригодность их для ведения конфиденциальных работ Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных изделий и документов. Организация защиты информации при осуществлении рекламной и публикаторской деятельности. Организация защиты информации при подготовке материалов к открытому опубликованию		
Самостоятельная работа обучающегося 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, содержащимикоммерческую 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 объектовый 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.	**50**	**3**

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 публикаторской 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 публикаторской деятельности и связей с прессой; участие в ней 17. Службы безопасности 18. Методы оценки эффективности защитных мероприятий в рекламной и публикаторской 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		

24. Составление списков участников совещания 25. Определение состава информации, используемой в ходе совещаний, переговоров		
Учебная практика **Виды работ** 1.Выполнение анализа и обработки распорядительных документов; 2. Проведение исследований документов, регламентирующих работу по защите информации; 3. Ведение делопроизводства с учетом конфиденциальности информации; 4. Проектирование электронной передачи данных, конструктивно-технологических модулей с применением пакетов прикладных программ; 5. Разработка комплекта документации; 6. Определение показателей надежности и оценка качества хранения конфиденциальных документов на различных носителях; 7. Разработка проектной документации с использованием современных пакетов прикладных программ в сфере профессиональной деятельности; 8. Инвентаризация объектов, подлежащих защите; 9. Изучение требований отчетной документации, используемой при сборе, обработке и передаче конфиденциальной информации; 10. Определение всех необходимых правовых документов связанных с защитой информации; 11. Выявление методов защиты объектов; 12. Сбор материала, необходимого для выработки решений по обеспечению защиты информации; 13. Анализ материала для выработки оптимальных решений по обеспечению защиты информации; 14. Выявление возможных каналов утечки конфиденциальной информации;	**36**	

15. Выявление зон доступа по типу и степени конфиденциальности работ; 16. Использование критериев подбора и расстановки сотрудников подразделений защиты информации 17.Изучение требований к процессу проведения инструктажа персонала по организации работы с конфиденциальной информацией;		
Производственная практика(по профилю специальности) **Виды работ** 1. Разработка должностной инструкции охранника объекта 2. Разработка должностной инструкции начальника охраны объекта 3. Подготовка проекта установки камер внешнего видеонаблюдения объекта 4. Подготовка проекта установки камер внутреннего видеонаблюдения объекта 5. Составление технического регламента работы с конфиденциальной информацией для персонала, имеющего допуск к конфиденциальной информации 6. Составление технического регламента о порядке оформления допуска лиц к конфиденциальным сведениям 7. Составление технического регламента работы с системой внешнего видеонаблюдения 8. Составление технического регламента работы с системой внутреннего видеонаблюдения 9. Составление технического регламента организации и проведения рабочих совещаний 10. Подготовка проекта выделения зон доступа по типу работ на объекте 11. Подготовка проекта выделения зон доступа по конфиденциальности работ объекте 12. Подготовка проекта установки СКУД на объекте 13. Составление технического регламента работы с СКУД объекта	**108**	

14. Составление Положения об охране персонала объекта 15. Составление Положения о режимных помещениях объекта 16. Подготовка проекта оборудования режимного помещения объекта 17. Составление технического регламента организации и проведения совещаний по конфиденциальным вопросам 18. Составление Положения о защите информации при приеме посетителей на объекте 19. Составление Положения о процедуре служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией 20. Составление Положения об организации работы при осуществлении международного сотрудничества 21. Составление технического регламента контроля соблюдения персоналом требований режима защиты информации на объекте 22. Проведение исследования о целесообразности внедрения биометрических систем безопасности на объекте 23. Проведение технического аудита системы видеонаблюдения объекта 24. Проведение технического аудита СКУД объекта 25. Проведение технического аудита безопасности компьютерных систем объекта 26. Составление Положения о подразделении защиты информации 27. Составление Положения о проверке персонала по защите информации 28. Составление технического регламента работы с компьютерными системами объекта 29. Составление технического регламента защиты информации в процессе рекламной деятельности 30. Проведение технического аудита организации охраны объекта 31. Проведение исследования о соответствии подбора и расстановки сотрудников подразделений защиты		

информации		

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1.- ознакомительный (узнавание ранее изученных объектов, свойств)
2.- репродуктивный (выполнение деятельности по образцу, инструкции и под руководством)
3. -продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Материально-техническое обеспечение

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. Партыка Т.Л., Попов И.И. Информационная безопасность. М.:Форум,2013
2. Аксеров Т.М. Защита информации и информационная безопасность. М.:Рос.экон.акад.,2012
3. Колмогоров А.Н. Безопасность предприятия. М.:Академия, 2014
4. Васильева И.Н., Стельмашонок Е.В. Информационные технологии и защита информации. Учебное пособие. - СПб, СПбГИЭУ,2012
5. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. Учебное пособие. - М.: Форум: Инфра-М, 2013.
6. В.И. Аверченков, М.Ю. Рытов. Организационная защита информации: учеб.пособие. М. : Флинта, 2013. - 184 с.
7. О.А. Романов, С.А. Бабин, С.Г. Жданов. Организационное обеспечение информационной безопасности: учебник. М.: Академия, 2012. - 192 с.

Дополнительные источники:

1. 1 Собрание законодательства РФ от 20 февраля 1995. Федеральный закон «Об информации, информатизации и защите информации». М.: «Юридическая литература», 2012
2. Васильева И.Н. Защита информации. СПб.:СПбГИЭУ, 2012
3. Гаценко О.Ю. Защита информации. СПб.: Изд. дом "Сентябрь", 2013.
4. В.П. Мельников, С.А. Клейменов. Информационная безопасность и защита информации. М.: Академия, 2012. - 336 с.
5. С.П. Расторгуев. Основы информационной безопасности. М.: Академия, 2012. - 192

Интернет-ресурсы:

1. Федеральный портал «Российское образование» - http: //www. edu.ru/

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

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.	- определение методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации; - выполнение анализа научной литературы; - обоснование выбора сооветствующихся решений по защите информации объекта; - обоснование использованных методов обнаружения технических каналов утечки информации	Текущий контроль: - ситуационные задачи, - практические работы, - самостоятельная работа, - защита работ на различных этапах производственной практики, - тестирование.
ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте	- определение предложений по разработке программ защиты информации на объекте; - определение методик защиты информации на предприятии	
ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации	- выполнение работ по защите конфиденциальной информацией; - определение качества защиты информации; - выполнение мероприятий по комплексной защите информации	
ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональнойдеятельности	- обоснование выбранных организационных решений на объектах информатизации; - обоснование мер по внедрению организационных решений на предприятии;	
ПК 1.5. Вести учет, обработку,	-обоснование	

хранение, передачу, использование различных носителей конфиденциальной информации	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	
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.	
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.	
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.	
ПК 1.9. Участвовать в оценке	- выполнение оценки	

качества защиты объекта	качества комплексной защиты информации организации; - выполнение оценки качества защиты объекта информатизации; - определение и анализ недостатков качества защиты информации напредприятии	

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только формирование 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**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.	- демонстрация понимания целей и задач профессиональной деятельности; - осознание способов деятельности, выбор средств, адекватных ее целям и задачам	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методов и способов решения профессиональных задач в организации и технологии защиты информации; - оценка эффективности и качества выполнения работ.	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- рациональность решения стандартных профессиональных задач в области защиты информации; - аргументированность самоанализа выполнения профессиональных задач	
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и	- эффективный поиск необходимой информации; - использование различных источников, включая электронные;	

личностного развития.		
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	- 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, 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), 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 профессиональногомодуля	
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	- анализ инноваций в области защиты информации	
ОК 10. Применять математический аппарат для решения профессиональных задач.	- применение математического анализа для решения профессиональных задач	
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.	- самостоятельная оценка значимости документов, применяемых в профессиональной деятельности	
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	- анализ структуры федеральных органов исполнительной власти, обеспечивающих информационную безопасность	