Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение

«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО
На заседании педагогического совета
Протокол № 3
«05» июля 2022г

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ 1. Участие в планировании и организации работ по обеспечению защиты объекта

для специальности 10.02.01 «Организация и технология защиты информации»

среднего профессионального образования

(базовой подготовки)

Санкт- Петербург2022 г.

ОДОБРЕНА
Цикловой комиссией
Общетехнических дисциплин
и компьютерных технологий
Протокол № 9
от «24» мая 2022 г.


_____Андреев В.В.

РАССМОТРЕНА
Методическим советом
«АУГСГиП»
Протокол № 6
от «28» июня 2022 г.

Рабочая программа профессионального модуля ПМ.01. Участие в планировании и организации работ по обеспечению защиты объекта разработана на основе Федерального государственного образовательного стандарта по специальности 10.02.01 «Организация и технология защиты информации»

Разработчик:

Белова С.В., преподаватель СПб ГБПОУ «Академия управления городской средой, градостроительства и печати»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля *ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта* является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО *10.02.01 Организация и технология защиты информации* 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. Участвовать в разработке программ и методик организации защиты информации на объекте.

ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.

ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.

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

ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.

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

ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.

ПК 1.9. Участвовать в оценке качества защиты объекта.

Рабочая программа профессионального модуля может быть использована при разработке программы по дополнительному профессиональному образованию и профессиональной подготовке в области подготовки специалистов.

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

С целью овладения указанным видом профессиональной деятельности 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 инструктажперсонала 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;
- 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:

всего – **696** часа, в том числе:
максимальной учебной нагрузки обучающегося – **480** часов, включая:
обязательной аудиторной учебной нагрузки обучающегося – 320 часов;
самостоятельной работы обучающегося – **160** часов;
учебной практики – 108 часа;
производственной практики - 108 часов.

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.	Участвовать в разработке программ и методик организации защиты информации на объекте.
ПК 1.3	Осуществлять планирование и организацию выполнения мероприятий по защите информации.
ПК 1.4	Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.
ПК 1.5	Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.
ПК 1.6	Обеспечивать технику безопасности при проведении организационно- технических мероприятий.
ПК 1.7	Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.
ПК 1.8	Проводить контроль соблюдения персоналом требований режима защиты информации.
ПК 1.9	Участвовать в оценке 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), 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 профессиональных задач.
ОК 11	Оценивать значимость документов, применяемых в профессиональной деятельности.
ОК 12	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

Перечень личностных результатов

Код	Наименование личностных результатов
ЛР 1	Осознающий себя гражданином и защитником великой страны.
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.
ЛР 3	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 5	Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.
ЛР 6	Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях.
ЛР 7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
ЛР 8	Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства.
ЛР 9	Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.
ЛР 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11	Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.
ЛР 12	Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания.
ЛР 13	Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности.
ЛР 14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.
ЛР 15	Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта

3.1. Тематический план профессионального модуля «ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта»

Коды профессиональных компетенций	**Наименования разделов профессионального модуля**	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная,** часов
			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**	
ПК 1.1 - ПК 1.9	МДК 01.01 Обеспечение организации системы безопасности предприятия	**180**	120	36	20	**60**	10	36	**36**
	МДК 01.02 Организация работ подразделений защиты информации	**150**	100	30		**50**		36	**36**
	МДК.01.03 Организация работы персонала с конфиденциальной информацией	**150**	100	30		**50**		36	**36**
	УП.01 Учебная по ПМ.01	**108**							
	ПП.01 Производственная по ПМ.01	**108**							
ВСЕГО		**696**	**320**	**96**	**20**	**160**	**10**	**108**	**108**

3.2. Содержание обучения по профессиональному модулю ПМ.01 Участие 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, курсовая работа (проект) (если предусмотрены)	Объем часов	Уровень освоения
Раздел 1. Организация системы безопасности предприятия			
МДК.01.01 Обеспечение организации системы безопасности предприятия			
Введение	**Содержание учебного материала**	**12**	
Тема 1. Сущность и задачи комплексной защиты информации предприятия	**Предмет, цели и задачи и содержание междисциплинарного курса.** Структура МДК. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия. **Понятийный аппарат в области обеспечения безопасности информации.** Общие понятия информации, безопасности информации, защиты информации и конечных целей защиты.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14
	2. Цели, задачи и принципы построения комплексной системы защиты информации. Понятие целей и задач КСЗИ. Принципы КСЗИ. Принцип системности. Принцип комплексности. Принцип своевременности. Принцип непрерывности. Принцип разумной достаточности. Принцип простоты применения.	2	
	Система физической защиты предприятия и основы ее организации. Принцип разумной достаточности при организации СФЗ предприятия. Зависимость состояния защищенности от уровня экономического развития организации. Обоснование экономической эффективности КСФЗ.	2	
	Управление системой физической защиты предприятия. Разработка концепции управления безопасности предприятием, как фактор, влияющий на построение КСЗИ. Основные положения нормативно- методических документов.	2	
	Цели и задачи системы охраны, пропускного и внутри объектового режима.	2	

	Системно-концептуальный подход к организации охраны предприятия. Влияние и внутри объектового режима как основных элементов системы информационной безопасности.		
	Современное понимание методологии защиты информации. Особенности национального технического регулирования. Система стандартов в области информационной безопасности. Система сертификации деятельности ФСТЭК России.	2	
Тема 2. Принципы организации и этапы разработки комплекснойзащиты информации (КСЗИ)	**Содержание учебного материала.**	**12**	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Методологические основы организации КСЗИ. Направления работ по созданию КСЗИ. Комплексные задачи, решаемые методологическим аппаратом.	2	
	Разработка политики безопасности и регламента безопасности организации. Планирование безопасности организации. Политика безопасности, как документ верхнего уровня. Соблюдение принципа разумной достаточности. Регламент безопасности, как документ, регламентирующий правила обращения с конфиденциальной информацией в зависимости от фазы ее обработки и категории конфиденциальности.	2	
	3. Основные положения отраслевых концепций информационной безопасности. Базовые понятия, состав и основное содержание отраслевых концепций информационной безопасности.	2	
	Система управления информационной безопасностью организации. Принципы построения и взаимодействие с другими подразделениями. Состав системы управления информационной безопасностью организации (СУИБ). Структура системы управления безопасностью информации и отдела обеспечения безопасности информации. Основные направления деятельности СУИБ.	2	
	Требования, предъявляемые к КСЗИ. Требования к организационной и технической составляющим КСЗИ. Требования по безопасности, предъявляемые к изделиям ИТ: порядок задания требований, разработка изделия ИТ, обеспечение поддержки доверия к безопасности изделия ИТ при эксплуатации, Подтверждение соответствия изделий ИТ требованиям безопасности	2	

	информации, поставка и ввод в действие, эксплуатация объекта.		
	6. Этапы разработки КСЗИ. Концептуальные подходы к проектированию систем информации организации: «продуктовый», «комплекс продуктов», комплексный». Этапы по созданию КСЗИ: обследование организации, проектирование системы защиты информации. Внедрение системы защиты информации, сопровождение системы информационной безопасности, обучение специалистов по защите информации.	2	
	Практические занятия	**2**	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
	№1 Разработка политики безопасности организации	2	
Тема 3. Факторы, влияющие на организацию комплексной системы защиты информации	**Содержание учебного материала.**	**8**	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14
	1. Персонал предприятия как носитель защищаемой информации. Организация работы с персоналом предприятия, система допуска к информации, ответственность за неправомерное разглашение информации.	2	
	2. Характер основной деятельности предприятия. Классификация предприятий по виду деятельности. Специфические особенности КСЗИ организации, связанные с и проведением организационных, правовых и технических мероприятий защиты информации.	2	
	3. Состав, объекты и степень конфиденциальности защищаемой информации. Основные особенности защиты информации в зависимости от состава защищаемой информации: государственная тайна, служебная тайна, коммерческая тайна, персональные данные.	2	
	Структура и задачи, решаемые предприятием. Классификация предприятий по их структуре, влияющая на определение параметров КСЗИ. Влияние внешнеэкономической и рекламной деятельности на организациюзащиты информации.	2	
	Практические занятия и лабораторные работы	**2**	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
	№2 Разработка концепции безопасности предприятия	2	
Тема 4. Определение и нормативное закрепление состава защищаемой информации	**Содержание учебного материала.**	**4**	
	Классификация информации по видам тайны и степеням конфиденциальности. Классификация информации в зависимости от порядка предоставления или распространения. Классификация информационных ресурсов по категориям доступа.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14
	2. Нормативно-правовые аспекты определения состава защищаемой информации. Задачи, влияющие на определение состава защищаемой	2	

	информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия.		
	Практические занятия и лабораторные работы	**2**	
	№3 Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия	2	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
Тема 5. Определение объектовзащиты	**Содержание учебного материала.**	**4**	
	1. Значение носителей защищаемой информации как объектов защиты. Носители информации как объект правовых отношений. Носители информации как возможный источник ее утечки. Требования по защите документированной информации.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14
	2. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации.	2	
	Практические занятия и лабораторные работы	**2**	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
	№4 Изучение методики выявления состава носителей защищаемой информации	2	
Тема 6. Дестабилизирующие воздействия на информацию и их нейтрализация	**Содержание учебного материала.**	**4**	
	1. Факторы, создающие угрозу информационной безопасности. Количественная недостаточность системы защиты. Качественная недостаточность системы защиты. Отказы. Сбои. Ошибки операторов АС. Стихийные бедствия. Злоумышленные действия. Побочные явления. Объективные и субъективные факторы.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14
	Обеспечение безопасности информации в непредвиденных ситуациях. План действий в непредвиденных ситуациях. Проведение обучения по действиям в непредвиденных ситуациях. Выделение мест резервного хранения информации. Резервирование телекоммуникационных услуг. Разработка требований по восстановлению ИТ.	2	
	Практические занятия и лабораторные работы	**2**	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
	№5 Угрозы безопасности информации	2	
Тема 7. Определение потенциальных каналов и методов несанкционированного доступа к информации	**Содержание учебного материала.**	**2**	
	Технические каналы утечки информации, их классификация. ТКУИ, как один из определяющих факторов несанкционированного доступа к информации. Классификация ТКУИ по способу перехвата информации и физической природе сигналов- переносчиков информации.	2	ОК 1,4,5,11,12;ПК 1.1.-1.3; ЛР 1-3,5,12,14

	Особенности защиты речевой информации Защита речевой информации: в выделенном помещении, предназначенном для ведения конфиденциальных переговоров, в кабинетах руководства предприятия; на абонентском участке телефонной линии; на всем протяжении телефонной линии.		
	Практические занятия и лабораторные работы	**8**	
	№6 Технические каналы утечки информации	2	
	№7 Защита информации от утечки по акустическому каналу пассивными методами	2	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
	№8. Исследование методов противодействия наблюдению	4	
Тема 8. Определение возможностей несанкционированного доступа кзащищаемой информации	**Содержание учебного материала.**	**4**	
	Методы и способы защиты информации. Методы защиты данных: препятствия, маскировка, регламентация, побуждение, принуждение. Формальные и неформальны средства защиты данных.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14
	2. Классификация средств защиты информации НСД. Классификация СЗИ НСД: по месту применения, по объектам защиты отдельного компьютера, по функциональному назначению.		
	Механизмы обеспечения безопасности информации от НСД. Идентификация и аутентификация. Разграничение доступа. Регистрация и аудит. Криптографическая подсистема. Межсетевое экранирование.		
	Практические занятия и лабораторные работы	**4**	
	№9 Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации	2	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
	№10 Изучение программных продуктов защиты информации	2	
Тема 9. Определение компонентов комплексной системы защиты информации предприятия	**Содержание учебного материала.**	**2**	
	1. Особенности синтеза СЗИ автоматизированных систем от НСД. Методика синтеза средств защиты информации. Выбор структуры СЗИ автоматизированной системы. Общее описание архитектуры автоматизированных систем, системы защиты информации и политики безопасности. Формализация описания архитектуры исследуемой автоматизируемой системы. Формулирование требований к системе защиты информации. Выбор механизмов и средств защиты информации. Определение важности параметров средств защиты информации. Линейная, кольцевая,	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3;ЛР 1-3,5,12,14

	сотовая, многосвязная и звездная структуры СЗИ АС.		
	Практические занятия и лабораторные работы	**2**	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
	№11 Оптимальное построение системы защиты для автоматизированной системы	2	
Тема 10. Определение условий функционирования комплексной системы защиты информации предприятия	**Содержание учебного материала.**	**2**	
	Содержание концепции построения КСЗИ. Объекты защиты. Цели и задачи обеспечения безопасности информации. Основные угрозы безопасности АС организации. Основные положения технической политики в области обеспечения безопасности информации АС организации. Основные принципы построения КСЗИ. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Первоочередные мероприятия по обеспечению безопасности информации АС предприятия.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3;ЛР 1-3,5,12,14
	Практические занятия и лабораторные работы	**2**	
	№12 Успешность реализации политики безопасности	2	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
Тема 11. Принципы и методы планирования функционирования комплексных систем защиты информации предприятия	**Содержание учебного материала.**	**2**	
	Понятие и задачи планирования функционирования КСЗИ. Способы и стадии планирования. Планирование функционирования как процесс. Этапы планирования. Фазы планирования. Уяснение задачи и оценка обстановки. Выработка замысла. Замысел. Завершение работы по принятию решения. Завершение планирования. Оформление и доведение документов планирования.	2	ОК 1,4,5,11,12;ПК 1.1.-1.3;ЛР 1-3,5,12,14
	Основы подготовки и принятия решений при планировании. **Методы сбора, обработки и изучения информации, необходимой для планирования.** Технология принятия управленческих решений. Уровни подготовки и принятия решений. Формальное преобразование информации. Содержательное преобразование информации. Коммуникационное преобразование информации. Временное преобразование информации. Автоматизированная система информационной поддержки ППР.		
	Практические занятия и лабораторные работы	**4**	ОК2,3,7,8,10;ПК1.4.-1.7.,1.9;ЛР1,6,7,15
	№13 Характеристика объектов защиты	2	
	№14 Построение модели объекта защиты	2	
Тема 12. Сущность и	**Содержание учебного материала.**	**4**	

содержаниеконтроля функционирования комплексной системы защиты информации предприятия	**Виды контроля функционирования КСЗИ. Цель проведения контрольных мероприятий в КСЗИ.** Основные требования к контролю. Общие цели контроля. Современные виды контроля. Внешний и внутренний контроль. Основные задачи контроля. Направления контроля состояния защиты информации. Принципы системы контроля состояния защиты информации. Функции органа контроля.	2	ОК 1,4,5,11,12;ПК 1.1.-1.3;ЛР 1-3,5,12,14
	2. **Анализ и использование результатов проведения контрольных мероприятий.** Периодичность проведения проверок технической защиты информации. Нарушения в области технической защиты информации. Содержание контроля состояния технической защиты информации. Контроль деятельности по технической защите информации. Контроль эффективности защиты.	2	
Тема 13. Управление комплексной системой защитыинформации в условиях чрезвычайных ситуаций	**Содержание учебного материала.**	**2**	
	Понятие и основные виды чрезвычайных ситуаций в организации.	2	ОК 1,4,5,11,12;ПК 1.1.-1.3;ЛР 1-3,5,12,14
	Технология принятия решений в условиях чрезвычайныхситуаций		
	Факторы, влияющие на принятие решений в условиях чрезвычайных ситуаций. Неопределенность. Ограниченность во времени. Физио-психологическое состояние лиц, принимающих решения и их исполнителей		
	Подготовка мероприятий на случай возникновения чрезвычайных ситуаций.		
Тема 14. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации организации	**Содержание учебного материала.**	**2**	
	Вероятностный подход. Оценочный подход.	2	
	Практические занятия и лабораторные работы	**4**	
	№15 Определение эффективности комплексной системы защиты информации	4	ОК 1,4,5,11,12;ПК 1.1.-1.3;ЛР 1-3,5,12,14
Тема 15. Методы и модели оценки эффективности комплексной системы защиты информации	**Содержание учебного материала.**	**2**	
	Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Метод относительного ранжирования. Личный опрос. Заочный опрос. Групповые методы опроса. Метод комиссии. Метод суда. Метод мозговой атаки. Синектика. Метод Дельфы.	2	ОК 1,4,5,11,12;ПК 1.1.-1.3;ЛР 1-3,5,12,14
	2. Экономический подход к оценке эффективности КСЗИ. Определение размеров ущерба с использованием моделей «осведомленность —		

	эффективность. Определение размеров ущерба с использованием экспертных оценок.		
	Практические занятия и лабораторные работы	**2**	ОК 2,3,7,8, 10;ПК1.4.-1.7., 1.9;ЛР 1,6,7,15
	№16 Определение затрат на защиту информации.	2	
Самостоятельная учебная работа при изучении раздела 1. МДК.01.01 Обеспечение организации системы безопасности предприятия Понятия безопасности и защищенности (презентация). Служебная и коммерческая тайны - сравнительная характеристика (презентация). Основные требования ФСТЭК России по защите персональных данных (презентация). Подходы зарубежных стран к защите конфиденциальной информации (доклад). Порядок разработки Перечня сведений, составляющих коммерческую тайну, внесение в него изменений идополнений (презентация). Основные источники защищаемой информации (презентация). Интеллектуальная собственность предприятия как объект защиты (презентация). Необходимость защиты «ноу-хау» (презентация). Категории доступа помещений предприятия для работы с защищаемой информацией (презентация). Объективные и субъективные факторы, создающие угрозу информационной безопасности (презентация). Описание каналов утечки информации (презентация) Задачи КСЗИ по выявлению угроз и каналов утечки информации (презентация). Классификация методов и средств защиты данных (презентация). Общее содержание работ по организации КСЗИ (презентация). Основные направления развития и совершенствования МТО ЗИ (презентация). Перечень основных внутренних организационно-распорядительных документов по организации защиты персональных данныхорганизации (презентация). Анализ технических средств охраны для оборудования режимных помещений (презентация). Анализ технических средств и систем контроля доступа на режимные территории (презентация). Принципы управления КСЗИ: комплексность, своевременность, непрерывность, активность, законность, обоснованность, специализация, взаимодействие и координация, централизация управления (сравнительный анализ). Основные методы контроля, виды контроля эффективности защиты (реферат). Определение упущенной выгоды в результате ограничений на распространение информации (реферат). Требования основных нормативно-методических документов ФСТЭК России (СТР-К, ГОСТ) в области информационной безопасности (презентационные доклады).		**60**	ОК 2,3,7,8, 10;ПК1.4.-1.7., 1.9;ЛР 1,6,7,15
Курсовой проект		**20**	

(работа) МДК 01.01Обеспечение организации системы безопасности предприятия			
	1. Выдача тем курсовой работы. Требования к оформлению курсовой работы.	2	ОК 1,4,5,11, 12; ПК 1.1.-1.3; ЛР 1-3,5,12, 14,15.
	2. Составление плана работы.	2	
	3. Работа над основной частью.	6	
	4. Оформление введения и заключения.	2	
	5. Оформление списка использованной литературы.	2	
	6. Оформление приложений к работе.	2	
	7. Защита курсовой работы.	4	
	Всего:	**180**	
Раздел 2. Работа подразделенийзащиты информации.			
МДК.01.02 Организация работ подразделений защиты информации		**2**	
Введение	Предмет, цели, задачи и содержание междисциплинарного курса Значение и место курса в подготовке кадров по специальности «Организация и технология защиты информации». Структура МДК. Базовые знания, необходимые для изучения курса.	2	ОК 1,4,5, 11,12;ПК 1.1.-1.3; ЛР 8-11,14,15
Тема 1. Место и роль подразделений защиты информации в системе защиты информации.	**Содержание учебного материал.**	**10**	
	Назначение подразделений защиты информации.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Место подразделений защиты информации в системе безопасности предприятия.	2	
	Подразделения защиты информации как составная часть системы защиты.	2	
	Подразделения защиты информации как орган управления защитой информации	2	
	Подразделения защиты информации как координатор деятельности по обеспечению безопасности информации.	2	
Тема 2. Задачи и функции подразделений защиты информации.	**Содержание учебного материала.**	**2**	
	Организационные, технологические и координационные задачи и функции подразделений зашиты информации.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Практические занятия и лабораторные работы	**4**	
	№1 Служба защиты информации как координатор деятельности по обеспечению безопасности информации **№ 2** Организация службы защиты информации на предприятии.	2 2	ОК 2,3,7,8, 10; ПК1.4.-1.7.,1.9; ЛР 1,6,7,15
Тема 3. Структура и	**Содержание учебного материала.**	**6**	

штатыподразделений защиты информации.	Общая структурная схема подразделений защиты информации. Виды и типы организационных структур подразделений защиты информации.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Централизованная и децентрализованная структуры подразделений защиты информации, условия, критерии, определяющие выбор структур.	2	
	Должностной состав сотрудников подразделений защиты информации, его зависимость от характера выполняемых работ.	2	
	Практические занятия и лабораторные работы	**8**	
	№ 3 Факторы, влияющие на определение задач и функций службы защиты информации.	2	ОК 2,3,7,8,10; ПК1.4.-1.7.,1.9; ЛР 1,6,7,15
	№ 4 Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений защиты информации.	2	
	№ 5 Факторы, определяющие конкретную структуру подразделений защиты информации.	2	
	№ 6 Факторы, определяющие численность сотрудников подразделений защиты информации.	2	
Тема 4. Организационные основы и принципы деятельности подразделений защиты информации.	**Содержание учебного материала.**	**8**	
	Порядок создания подразделений защиты информации.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Структура и содержание положения о подразделениях защиты информации.	2	
	Состав и содержание других нормативных документов, регламентирующихдеятельность подразделений защиты информации.	2	
	Основные принципы организации и деятельности подразделений защиты информации.	2	
	Практические занятия и лабораторные работы	**6**	
	№ 7 Организационно-распорядительные документы по защите информации	4	ОК 2,3,7,8,10; ПК1.4.-1.7.,1.9; ЛР 1,6,7,15
	№ 8 Особенности подбора кадров	2	
Тема 5. Подбор, расстановка и обучение сотрудников подразделений защиты информации.	**Содержание учебного материала.**	**6**	
	Общие требования, предъявляемые к сотрудникам подразделений защиты информации.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Формы создания и способы поддержания необходимого микроклимата в коллективе.	2	
	Формы повышения квалификации сотрудников.	2	
	Практические занятия и лабораторные работы	**6**	

	№ 9 Отбор кандидатов и прием на работу сотрудников в подразделение защиты информации	6	ОК 2,3,7,8,10; ПК1.4.-1.7.,1.9; ЛР 1,6,7,15
Тема 6. Организация трудасотрудников подразделений защиты информации.	**Содержание учебного материала.**	**12**	
	Деятельность сотрудников подразделений защиты информации.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Структура и содержание должностных инструкций сотрудников подразделений защиты информации.	2	
	Организация рабочих мест сотрудников подразделений зашиты информации.	2	
	Оснащение оборудованием, техническими средствами рабочих мест сотрудников подразделений зашиты информации.	2	
	Обеспечение необходимых условий труда. Охрана труда.	2	
	Карты организации трудового процесса.	2	
Тема 7. Принципы и методы управления подразделений защиты информации	**Содержание учебного материала.**	**12**	
	Принципы управления подразделениями защиты информации.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Понятие и сущность методов управления. Система методов управления.	2	
	Административно-правовые методы управления. Экономические методы управления.	2	
	Социально-психологические методы управления.	2	
	Взаимосвязь методов управления.	2	
	Необходимость комплексного и системного применения методов управления службойзащиты информации.	2	
	Практические занятия и лабораторные работы	**2**	
	№10 Решение ситуационных задач по теме «Понятие и сущность методов управления подразделением защиты информации».	2	ОК 2,3,7,8,10; ПК1.4.-1.7.,1.9; ЛР 1,6,7,15
Тема 8. Технология управления подразделениями защиты информации	**Содержание учебного материала.**	**10**	
	Состав содержание управленческих функций.	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Технология управления подразделениями защиты информации.	2	
	Значение управленческих решений. Цели планирования. Виды планирования, их назначение.	2	
	Содержание и структура планов. Технология планирования. Методы и формы контроля выполнения планов	2	
	Критерии эффективности подразделений защиты информации.	2	

	Практические занятия и лабораторные работы	**4**	
	№11 Семинар на тему «Работа подразделенийзащиты информации» (обобщающее занятие)	4	ОК 2,3,7,8,10; ПК1.4.-1.7.,1.9; ЛР 1,6,7,15
Самостоятельная учебная работа при изучении раздела 2. МДК.01.02 Организация работ подразделений защиты информации 1. Статус подразделения защиты информации в структуре предприятия (доклад). 2. Организационные, технологические и координационные задачи и функции (сравнительный анализ). 3. Виды организационных структур подразделений защиты информации (презентация). 4. Ответственность заместителя руководителя предприятия по безопасности в области защиты информации (доклад). 5. Условия и факторы, влияющие на организацию работы подразделений защиты информации (презентация). 6. Специфические требования, предъявляемые к сотрудникам службы защиты информации (презентация). 7. Подготовка кадрового резерва (доклад). 8. Методика определения численного состава подразделений защиты информации (сообщение). 9. Культура труда (презентация). 10. Особенности приема сотрудников в подразделения защиты информации (презентация). 11. Особенности увольнения сотрудников подразделения защиты информации (презентация). 12. Общие принципы управления подразделениями защиты информации (сравнительный анализ). 13. Методы управления подразделениями защиты информации (сравнительный анализ). 14. Управленческие функции (презентация). 15. Изучение всех сторон коммерческой и другой деятельности для выявления и закрытия возможных каналов утечки информации. 16. Ведение учета и анализа нарушений режима безопасности, накопление и анализ данных о внеправовых действиях конкурентов.		**50**	ОК 1-3,7,8, 10-12; ПК 1.1.- 1.9; ЛР 1-6,7,15.
	Всего:	**150**	
Раздел 3. Работа персонала сконфиденциальной информацией.			
МДК.01.03 Организация работы персонала с конфиденциальной информацией			
Введение	Предмет, цели, задачи и содержание междисциплинарного курса Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.	**2**	ОК 1,4,5, 11,12; ПК 1.1.-1.3; ЛР 8-11,14,15
Тема 1. Общая	**Содержание учебного материала.**	**6**	

характеристика нормативно-правовой базы	Понятие и особенности конфиденциальной информации. Персональные данные.	2	ОК 1,4,5, 11,12; ПК 1.1.-1.3;
	Тайна следствия и судопроизводства. Служебная тайна. Профессиональная тайна. Коммерческая тайна.	2	
			ЛР 8-11,14,15
	Секрет производства и служебный секрет производств	2	
	Практические занятия и лабораторные работы	**8**	
	№1 Законодательство РФ в области информационной безопасности	8	ОК 1,4,5, 11,12; ПК 1.1.-1.3; ЛР 8-11,14,15
Тема 2 Документирование конфиденциальной информации	**Содержание учебного материала.**	**14**	
	Особенности документирования конфиденциальной информации	2	ОК 1,4,5,11, 12; ПК 1.1.-1.3; ЛР 1-3,5,12, 14.
	Определение степени ограничения доступа к документам и использование отметки конфиденциальности при оформлении документов	2	
	Разработка перечня конфиденциальной документированной информации	2	
	Учет бумажных носителей конфиденциальной информации	2	
	Учет проектов конфиденциальной документированной информации	2	
	Особенности создания и изготовления конфиденциальных документов с помощью средств ЭВТ, их печатания, тиражирования, размножения	2	
	Учет использования и хранения печатей, штампов, бланков, необходимых для оформления конфиденциальных документов	2	
	Практические занятия и лабораторные работы	**4**	
	№2 Разработка перечня документированной конфиденциальной информации на предприятии	2	ОК 2,3,7, 8, 10;ПК1.4. -1.7., 1.9;ЛР 1,6,7,15.
	№3 Организация системы доступа к конфиденциальным документам	2	
Тема 3. Организация конфиденциального документооборота	**Содержание учебного материала.**	**14**	
	Особенности учета и регистрации конфиденциальной документированной информации	2	ОК 1,4,5,11, 12; ПК 1.1.-1.3;
	Обработка поступающих конфиденциальных документов, их учет и регистрация	2	

	Учет и регистрация внутренних (созданных/изданных) конфиденциальных Документов	2	ЛР 1-3,5,12,14.
	Технологии исполнения и контроля за исполнением конфиденциальных документов	2	
	Учет и регистрация отправляемых (исходящих) конфиденциальных документов, их экспедиционная обработка и рассылка	2	
	Учет конфиденциальной документированной информации инвентарного (выделенного) хранения	2	
	Учет конфиденциальной информации при ее автоматизированной обработке	2	
	Практические занятия и лабораторные работы	**4**	
	№4 Порядок формирования конфиденциального дела.	2	ОК 2,3,7, 8, 10;ПК1.4. -1.7., 1.9;ЛР 1,6,7,15.
	№5 Проведение экспертизы ценности конфиденциальных документов	2	
Тема 4. Разрешительная система доступа к конфиденциальной информации	**Содержание учебного материала.**	**14**	
	Основные требования к разрешительной системе доступа	2	ОК 1,4,5,11, 12; ПК 1.1.-1.3; ЛР 1-3,5,12, 14.
	Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства и служебный секрет производства	2	
	Особенности доступа к конфиденциальной документированной информации при ее предоставлении уполномоченным органам государственной власти	2	
	Особенности доступа к конфиденциальной документированной информации, составляющей персональные данные	2	
	Особенности доступа к архивным конфиденциальным документам	2	
	Особенности доступа должностных лиц при их командировании к конфиденциальной документированной информации	2	
	Учет персонала, получившего доступ к конфиденциальной документированной информации, и (или) лиц, которым она была передана или предоставлена	2	
	Практические занятия и лабораторные работы	**2**	

	№6 Анализ положения о разрешительной системе доступа к конфиденциальной информации	2	ОК 2,3,7,8, 10; ПК1.4.-1.7., 1.9;ЛР 1,6,7,15.
Тема 5. Режим конфиденциальности документированной информации	**Содержание учебного материала.**	**6**	
	Режим обмена конфиденциальной документированной информацией. Режим сохранности конфиденциальных документов и дел	2	ОК 1,4,5,11, 12;ПК 1.1.-1.3; ЛР 1-3,5,12, 14.
	Режим конфиденциальности при проведении совещаний и переговоров	2	
	Проверка наличия носителей конфиденциальной информации	2	
	Практические занятия и лабораторные работы	**2**	
	№7 Учет персонала, получившего доступ к конфиденциальной документированной информации	2	ОК 2,3,7,8, 10;ПК1.4.-1.7.,
			1.9;ЛР 1,6,7,15.
Тема 6. Система защищенного электронного документооборота	**Содержание учебного материала.**	**12**	
	Особенности конфиденциального электронного документооборота. Основные виды угроз информационной безопасности организации.	2	ОК 1,4,5,11, 12; ПК 1.1.-1.3; ЛР 1-3,5,12,14.
	Основные требования и меры по защите конфиденциальной информации, циркулирующей в эксплуатируемой автоматизированной информационной системе	2	
	Организация работ при создании системы защиты электронного документооборота. Организация проведения работ по защите конфиденциальной информации при ее автоматизированной обработке	2	
	Обеспечение контроля защиты электронного документооборота	2	
	Аттестация автоматизированных информационных систем по требованиям безопасности информации	2	
	Защита от вредоносных программ. Защита системы электронных сообщений.	2	
	Практические занятия и лабораторные работы	**10**	
	№8 Технические мероприятия при проведении совещаний и переговоров. Способы предотвращения подслушивания и наблюдения при проведении совещаний и переговоров.	2	ОК 2,3,7,8, 10; ПК1.4.-1.7., 1. ЛР 1,6,7,15.
	№9 Проведения аудита состояния информационной безопасности предприятия	2	
	№10 Составление плана мероприятий по защите информации при подготовке к проведению совещания.	2	
	№11 Изучение программных продуктов защиты информации	2	

№12 Успешность реализации политики безопасности	2	
Самостоятельная учебная работа при изучении раздела 3. МДК.01.03 Организация работы персонала с конфиденциальной информацией 1. Законы РФ «О коммерческой тайне», «Об информации, информатизации и защите информации», «О персональных данных» (доклад) 2. Нормативно-методическая база организации работы с документами, содержащими служебную тайну (доклад) 3. Сущность и принципы ограничения доступа к информации и документам (доклад) 4. Нормативно-правовые основы организации работы с документами, содержащими коммерческую тайну (доклад) 5. Создание и изготовление конфиденциальных документов с помощью ЭВМ их печатания, тиражирования и размножения. (доклад) 6. Учет использования и хранения печатей, штампов, бланков, необходимых для оформления	**50**	ОК 1-3,7,8, 10-12; ПК 1.1.- 1.9; ЛР 1-6,7,15.

документов (доклад) 7. Понятие "внутри объектовый режим". Его основное назначение при ведении конфиденциальных работ и обращении с охраняемымиизделиями и документами (доклад) 8. Порядок определения перечня предметов, запрещенных к проносу провозу на режимную территорию. Общие требования внутриобъектового режима. (доклад) 9. Экспедиционные технологии обработки и учета поступающих пакетов с конфиденциальной информацией (доклад) 10. Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта. (доклад) 11. Порядок допуска работников в помещения, где ведутся конфиденциальные работы. (доклад) 12. Организация работы по защите информации при осуществлении публицистической деятельности и связей с прессой; участие в ней Службы безопасности. (доклад) 13. Организация контроля за выполнением распорядка дня лицами, работающими на режимных объектах. (доклад) 14. Создание отдельных (выделенных) производственных зон (зон доступа) по типу и степени конфиденциальности работ ссамостоятельными системами организации и контроля доступа. (доклад) 15. Методика проектирования системы пропускного и внутри объектового режимов и оценки эффективности их функционирования. (доклад) 16. Методы оценки эффективности защитных мероприятий в рекламной и публицистической деятельности. (доклад) 17. Виды и способы охраны. Понятие о рубежах охраны. Многорубежная система охраны (доклад) 18. Порядок вывоза (выноса) материальных ценностей и документации с территории организации и ввоза (вноса) их на территорию (доклад) 19. Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта. (доклад) 20. Порядок допускаработников в помещения, где ведутся конфиденциальные работы (доклад) 21. Методика проектирования системы пропускного и внутри объектового режимов и оценки эффективности их функционирования (доклад) 22. Составление списков участников совещания. Определение состава информации, используемой в ходе совещаний, переговоров (доклад)		
Всего:	**150**	
Учебная практика:		
Виды работ: 1. Выполнение анализа и обработки распорядительных документов; 2. Проведение исследований документов, регламентирующих работу по защите информации;	**108**	

3. Ведение делопроизводства с учетом конфиденциальности информации; 4. Проектирование электронной передачи данных, конструктивно-технологических модулей с применением пакетов прикладныхпрограмм; 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 профессиональнойдеятельности; 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; 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:		
Виды работ: 1. Изучение организации охраны персонала, территорий, зданий, помещений и продукции предприятий; 2. Изучение техники использования аппаратной системы контроля доступа; 3. Изучение способов выделения зон доступа по типу и степени конфиденциальности работ; 4. Определение порядка организации и проведения рабочихсовещаний; 5. Изучение использования методов защиты информации в рекламной и выставочной деятельности; 6. Изучение и использование критериев подбора и расстановки сотрудников подразделений защиты информации; 7. Изучение организации работы с персоналом, имеющим доступ к конфиденциальной информации; 8. Изучение порядка проведения инструктажа персонала по организации работы с конфиденциальной информацией. 9. Изучение процесса контроля соблюдения персоналом требований режима защиты информации. 10. Изучение требований при выполнении мероприятий по защите информации; 11. Установление степени конфиденциальности информации для методов обработки, хранения,	**108**	

использования и передачи носителей; 12. Учет носителей конфиденциальной информации; 13. Проведение организационно-технических мероприятий; 14.Составление и соблюдение графика проведения проверок; 15. Выявление документов, подлежащих проверке; 16. Применение различных способов контроля персонала с целью соблюдения требований режима защиты информации; 17. Провести анализ носителей информации, применяемых на предприятии.		
Всего	**696**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие кабинета информационной безопасности; лаборатории технических средств защиты информации, программно-аппаратных средств защиты информации;

Оборудование учебного кабинета:

- рабочее место преподавателя;
- комплект учебно-методической документации;
- рабочие места по количеству обучающихся;
- наглядные пособия (таблицы, схемы и т.д.).

Технические средства обучения:

- компьютер;
- видеопроектор;
- интерактивная доска

Оборудование лаборатории технических средств защиты информации:

- посадочные места, рассчитанные на подгруппу, но не менее 8;
- мультимедийные средства обучения;
- рабочее место преподавателя;
- компьютеры с лицензионным программным обеспечением;
- специализированное программное обеспечение;
- системы доступа;
- программно-аппаратные средства защиты информации.

Оборудование лаборатории программно-аппаратных средств защиты информации:

- посадочные места, рассчитанные на подгруппу, но не менее 8;
- мультимедийные средства обучения.
- рабочее место преподавателя;
- компьютеры с лицензионным программным обеспечением.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

МДК 01.01 ОБЕСПЕЧЕНИЕ ОРГАНИЗАЦИИ СИСТЕМ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Основная литература

Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2022. — 592 с. — URL: http://znanium.com. — Режим доступа: по подписке.
Жук А. П. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. - 400 с. — URL: http://znanium.com. — Режим доступа: по подписке.
Казарин О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для СПО/ О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.
Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Дополнительная литература

Гришина Н. В. Информационная безопасность предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2019. — 239 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.
Тараскин М. М. Комплексная защита информации в организации : монография / М. М. Тараскин и др. — Москва : Русайнс, 2020. — 353 с. — URL: https://www.book.ru. — Режим доступа: по подписке.
Коваленко Ю.И. Методика защиты информации в организациях : монография / Ю.И. Коваленко, Г.И. Москвитин, М.М. Тараскин. — Москва : Русайнс, 2020. — 162 с. — URL: https://www.book.ru. — Режим доступа: по подписке.
Баранова Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 322 с. — URL: http://znanium.com. — Режим доступа: по подписке.
Баранова Е. К. Моделирование системы защиты информации. Практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 224 с. — URL: http://znanium.com. — Режим доступа: по подписке

МДК 01.02 ОРГАНИЗАЦИЯ РАБОТ ПОДРАЗДЕЛЕНИЙ ЗАЩИТЫ ИНФОРМАЦИИ

Основная литература

Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2022. — 592 с. — URL: http://znanium.com. — Режим доступа: по подписке.
Жук А. П. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. - 400 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.
Гришина Н. В. Основы информационная безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2023. — 216 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Дополнительная литература

Емельянова Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.
Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : ИД ФОРУМ : НИЦ ИНФРА-М, 2021. - 416 с.: ил. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.
Баранова Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — URL: http://znanium.com. — Режим доступа: по подписке.
Сычев Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 223 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

МДК 01.03 ОРГАНИЗАЦИЯ РАБОТЫ ПЕРСОНАЛА С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

Основная литература

Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - Москва : ИНФРА-М, 2022. - 256 с. — URL: http://znanium.com. — Режим доступа: по подписке.
Гугуева Т. А. Конфиденциальное делопроизводство : учебное пособие / Т.А. Гугуева. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2021. — 199 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.
Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. — URL: http://znanium.com. — Режим доступа: по подписке.
Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2022. — 592 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Дополнительная литература

Емельянова Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Кузнецов И. Н. Документационное обеспечение управления. Документооборот и делопроизводство : учебник и практикум для СПО / И. Н. Кузнецов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 462 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

4.3.Общие требования к организации образовательного процесса

Подготовка специалистов по модулю должна быть обеспечена учебно-методической документацией по всем разделам программы: методические руководства по выполнению практических и самостоятельных работ.

Каждый обучающийся должен иметь доступ к базам данных и библиотечным фондам. Во время самостоятельной подготовки обучающиеся должны быть обеспечены доступом к сети Интернет.

Учебные дисциплины, изучение которых предшествует освоению данного профессионального модуля:

ОП.04 Технические средства информатизации

ОП.05 Базы данных

ОП.06 Основы информационной безопасности

Профессиональный модуль содержит три междисциплинарных курса

МДК. 01.01. Обеспечение организации системы безопасности предприятия,

МДК 01.02. Организация работ подразделений защиты информации,

МДК. 01.03. Организация работы персонала с конфиденциальной информацией, в которых предусмотрено изучение теоретического материала, а также выполнение практических работ, которые проводятся в лабораториях техникума под руководством преподавателя. Для выполнения практических работ разрабатываются инструкционные карты. После каждого раздела предусмотрена внеаудиторная самостоятельная работа, направленная на расширение кругозора по изучаемой тематике.

По междисциплинарным курсам профессионального модуля предусмотрена промежуточная аттестация в форме дифференцированного зачета. Зачет может быть проведен в устной форме, выполнен в форме реферата или решения ситуационных задач, подтверждающих профессиональную компетентность обучающихся.

Промежуточная аттестация по учебной и производственной практике – дифференцированный зачет.

Учет учебных достижений обучающихся проводиться при помощи различных форм текущего контроля:

- тестовые задания;
- практические работы;
- контрольные работы;
- самостоятельная работа.

Оценка качества подготовки обучающихся осуществляется в двух направлениях:

- Оценка уровня освоения дисциплины;
- Оценка компетенций обучающихся.

По профессиональному модулю рабочей программой предусмотрена учебная и производственная практики.

Задачей производственной практики является:

- закрепление и совершенствование приобретенных в процессе обучения профессиональных умений обучающихся;
- развитие общих и профессиональных компетенций;

Производственная практика проводится концентрированно после освоения материала профессионального модуля. Обязательным условием допуска к производственной практике (по профилю специальности) в рамках профессионального модуля Участие в планировании и организации работ по обеспечению защиты объекта является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля.

По профессиональному модулю обучающимися выполняется курсовая проект.

При работе над курсовым проектом обучающимся оказываются консультации.

Обязательной формой промежуточной аттестации по профессиональному модулю является комплексный экзамен (квалификационный).

Экзамен (квалификационный) проверяет готовность обучающегося к выполнению указанного вида профессиональной деятельности и сформированность у него компетенций, определенных в разделе 2. Результаты освоения профессионального модуля.

Экзамен (квалификационный) проводится по окончании освоения программы профессионального модуля и представляет собой форму независимой оценки результатов обучения с участием работодателей. Условием допуска к экзамену (квалификационному) является успешное освоение

обучающимися всех элементов программы профессионального модуля – МДК, учебной и производственной практики.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу (курсам):

Педагогические кадры, обеспечивающие обучение по данному профессиональному модулю должны иметь высшее образование, соответствующее профилю профессионального модуля, опыт деятельности в организациях соответствующей профессиональной сферы, проходить дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже 1 раза в 3 года.

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**
ПК1.1 Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.	- грамотная организация сбораи обработки материалов; - эффективное использованиесредств обнаружения возможных каналов утечки конфиденциальной информации.	Экспертная оценка выполненной работы. Текущий контроль в форме: - защиты практическихработ; - контрольных работ потемам МДК. - наблюдение за выполнением практических работ. Текущий контроль; - Промежуточная аттестация; Защита курсового проекта. Комплексный экзамен по профессиональному модулю.
ПК1.2 Участвовать в разработкепрограмм и методик организации защиты информации на объекте.	- правильность использованияметодик организации защиты информации на объекте; -умение разрабатывать программы по защите информации на объекте.	
ПК1.3 Осуществлять планирование и организацию выполнения мероприятий по защите информации.	-грамотное планирование мероприятий по защите информации; - правильная организация выполнения мероприятий по защите информации.	
ПК 1.4 Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.	-соблюдение корпоративной этики; - умение принимать организационные решения на объектах профессиональной деятельности.	

ПК1.5 Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.	-грамотное ведение учета, обработки, хранения, передачи,использования различных носителей конфиденциальной информации.	
ПК1.6 Обеспечивать технику безопасности при проведении организационно-технических мероприятий.	- соблюдение техники безопасности при проведении	
	организационно-технических мероприятий.	
ПК1.7 Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.	- грамотная организация и проведение проверок объектовинформатизации, подлежащихзащите.	
ПК1.8 Проводить контроль соблюдения персоналом требований режима защиты информации.	- правильность проведения контроля соблюдения персоналом требований режима защиты информации.	
ПК1.9Участвовать в оценке качества защиты объекта.	- грамотная оценка качества защиты объекта.	

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 интереса к будущей профессии;	Экспертная оценка выполненной работы.Текущий контроль в форме: - защиты практическихработ; - контрольных работ потемам МДК. - наблюдение за выполнением практических работ.Зачеты по производственной практике и по каждому изразделов профессионального модуля. Зачеты и экзамены поМДК. Защита курсового проекта. Комплексный экзамен по профессиональному модулю.
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 области защиты информации предприятий; оценка эффективности и качества выполнения;	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	-решение стандартных и Нестандартных профессиональных задач в области защиты информации;	
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	-эффективный поиск необходимой информации, использование различных источников, включая электронные;	
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	