ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«САРОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ ИМЕНИ ДВАЖДЫ ГЕРОЯ
СОЦИАЛИСТИЧЕСКОГО ТРУДА БОРИСА ГЛЕБОВИЧА МУЗРУКОВА»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01 УЧАСТИЕ В ПЛАНИРОВАНИИ И ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОБЪЕКТА

для специальности среднего профессионального образования
10.02.01 Организация и технология защиты информации

.

2021 г.

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

Организация – разработчик: ГБПОУ СПТ им. Б.Г. Музрукова

Разработчик: И.В. Столяров, преподаватель ГБПОУ СПТ им. Б.Г. Музрукова

СОГЛАСОВАНО
Протокол № 1 от «20» 08 2021 г.
Председатель МК
_____ Е.Н. Маресева

УТВЕРЖДАЮ
Зам. директора по УР
_____ О.Н.Тарасова
«20» 08 2021 г.

СОДЕРЖАНИЕ

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

1.1. Область применения программы

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.

Программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в области организации и технологии защиты информации при наличии среднего общего образования.

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 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;
- методы проверки персонала по защите информации;
- процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией

1.3. Количество часов на освоение программы профессионального модуля:

всего – **972** часа, в том числе:
максимальной учебной нагрузки обучающегося – **756** часов, включая:
обязательной аудиторной учебной нагрузки обучающегося – **504** часа;
самостоятельной работы обучающегося – **252** часа;
учебной практики – **108** часов;
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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Код профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), 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	10
ПК 1.1-1.9	**Раздел 1** Организация системы безопасности предприятия	**252**	168	74	10	84			
	Раздел 2 Работа подразделений защиты информации**.**	**252**	168	74	10	84			
	Раздел 3. Работа персонала с конфиденциальной информацией.	**252**	168	74	10	84			
ПК 1.1-1.9	**Учебная практика**	**108**						108	
ПК 1.1-1.9	**Производственная практика, (по профилю специальности)**, часов	**108**							108
Всего:		**972**	**504**	**222**	**30**	**252**		**108**	**108**

3.2. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
Раздел 1. Организация системы безопасности предприятия			**252**	
МДК 01.01. Обеспечение организации системы безопасности предприятия			**252**	
Введение	1	**Предмет, цели и задачи и содержание междисциплинарного курса.** Структура МДК. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.	**2**	1
Тема 1.1. Сущность и задачи комплексной защиты информации предприятия	**Содержание учебного материала.**		**12**	1-2
	1	**Понятийный аппарат в области обеспечения безопасности информации.** Общие понятия информации, безопасности информации, защиты информации и конечных целей защиты.	2	
	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	
	3	**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	
	4	**Управление системой физической защиты предприятия.** Разработка концепции управления безопасности предприятием, как фактор, влияющий на построение КСЗИ. Основные положения нормативно- методических документов.	2	
	5	**Цели и задачи системы охраны, пропускного и внутриобъектового режима.** Системно-концептуальный подход к организации охраны предприятия. Влияние пропускного и внутриобъектового режима как основных элементов системы информационной безопасности.	2	
	6	**Современное понимание методологии защиты информации.** Особенности национального технического регулирования. Система стандартов в области информационной безопасности. Система сертификации деятельности ФСТЭК России.	2	
	Практические занятия.		**6**	2
	1	Общие понятия обеспечения безопасности информации	2	

	2	Цели, задачи и принципы построения КСЗИ	2	
	3	Система охраны, пропускного и внутриобъектового режима	2	
Тема 1.2. Принципы организации и этапы разработки комплексной защиты информации (КСЗИ)	**Содержание учебного материала.**		**12**	1-2
	1	**Методологические основы организации КСЗИ.** Направления работ по созданию КСЗИ. Комплексные задачи, решаемые методологическим аппаратом.	2	
	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	
	4	**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	
	5	**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 информации, поставка и ввод в действие, эксплуатация объекта.	2	
	6	**Этапы разработки КСЗИ.** Концептуальные подходы к проектированию систем защиты 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.		**6**	2
	1	Разработка политики безопасности и регламента безопасности организации	2	
	2	Требования к КСЗИ	2	
	3	Изучение этапов разработки КСЗИ	2	
Тема 1.3. Факторы, влияющие на организацию комплексной	**Содержание учебного материала.**		**8**	1-2
	1	**Персонал предприятия как носитель защищаемой информации.**	2	

системы защиты информации		Организация работы с персоналом предприятия, система допуска к информации, ответственность за неправомерное разглашение информации.		
	2	**Характер основной деятельности предприятия.** Классификация предприятий по виду деятельности. Специфические особенности КСЗИ организации, связанные с организацией 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	
	4	**Структура и задачи, решаемые предприятием.** Классификация предприятий по их структуре, влияющая на определение параметров КСЗИ. Влияние внешнеэкономической и рекламной деятельности на организацию защиты информации.	2	
	Практические занятия.		**4**	2
	1	Организация работы с персоналом предприятия	2	
	2	Конструктивные особенности организации, как фактор, влияющий на КСЗИ	2	
Тема 1.4. Определение и нормативное закрепление состава защищаемой информации	**Содержание учебного материала.**		**4**	1-2
	1	**Классификация информации по видам тайны и степеням конфиденциальности.** Классификация информации в зависимости от порядка предоставления или распространения. Классификация информационных ресурсов по категориям доступа.	2	
	2	**Нормативно-правовые аспекты определения состава защищаемой информации.** Задачи, влияющие на определение состава защищаемой информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия.	2	
	Практические занятия.		**4**	2-3
	1	Задачи, влияющие на определение состава защищаемой информации	2	
	2	Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия	2	
Тема 1.5. Определение объектов защиты	**Содержание учебного материала.**		**4**	1-2
	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	
	2	**Факторы, определяющие необходимость защиты периметра и здания предприятия.** **Особенности помещений как объектов защиты для работы по защите информации.**	2	
	Практические занятия.		**4**	2

	1	Изучение методики выявления состава носителей защищаемой информации	2	
	2	Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа	2	
Тема 1.6. Дестабилизирующие воздействия на информацию и их нейтрализация	**Содержание учебного материала.**		**4**	1-2
	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	
	2	**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.		**4**	2
	1	Угрозы безопасности информации	2	
	2	Модели нарушителей безопасности АС	2	
Тема 1.7. Определение потенциальных каналов и методов несанкционированного доступа к информации	**Содержание учебного материала.**		**4**	1-2
	1	**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	
	2	**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.	2	
	Практические занятия.		**8**	2-3
	1	Технические каналы утечки информации	2	
	2	Перехват информации по радиоканалу при использовании специальных технических средств	2	
	3	Вероятность обнаружения и распознавания объектов наблюдения по оптическому каналу	2	
	4	Средства видеонаблюдения и их установка	2	
Тема 1.8. Определение возможностей несанкционированного доступа к защищаемой информации	**Содержание учебного материала.**		**6**	1-2
	1	**Методы и способы защиты информации.** Методы защиты данных: препятствия, маскировка, регламентация, побуждение, принуждение. Формальные и неформальны средства защиты данных.	2	
	2	**Классификация средств защиты информации НСД.** Классификация СЗИ НСД: по	2	

		месту применения, по объектам защиты отдельного компьютера, по функциональному назначению.		
	3	**Механизмы обеспечения безопасности информации от НСД.** Идентификация и аутентификация. Разграничение доступа. Регистрация и аудит. Криптографическая подсистема. Межсетевое экранирование.	2	
	Практические занятия.		**4**	2-3
	1	Методы и способы защиты данных. Классификация СЗИ от НСД	2	
	2	Механизмы обеспечения безопасности информации	2	
Тема 1.9. Определение компонентов комплексной системы защиты информации предприятия	**Содержание учебного материала.**		**2**	1-2
	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, сотовая, многосвязная и звездная структуры СЗИ АС.	2	
	Практические занятия.		**2**	3
	1	Оптимальное построение системы защиты для автоматизированной системы	2	
Тема 1.10. Определение условий функционирования комплексной системы защиты информации предприятия	**Содержание учебного материала.**		**2**	1-2
	1	**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	
	Практические занятия.		**6**	2
	1	Определение основных условий функционирования КСЗИ	2	
	2	Основные угрозы безопасности информации АС организации	2	
	3	Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов	2	
Тема 1.11. Принципы и методы планирования функционирования комплексных систем защиты информации предприятия	**Содержание учебного материала.**		**4**	1-2
	1	**Понятие и задачи планирования функционирования КСЗИ. Способы и стадии планирования.** Планирование функционирования как процесс. Этапы планирования. Фазы	2	

		планирования. Уяснение задачи и оценка обстановки. Выработка замысла. Замысел. Завершение работы по принятию решения. Завершение планирования. Оформление и доведение документов планирования.		
	2	**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.	2	
	Практические занятия.		**12**	2-3
	1	Анализ мероприятий по ЗИ объекта	2	
	2	Разработка системы контроля вскрытия аппаратуры (СКВА) для заданного объекта	2	
	3	Построение модели объекта защиты	2	
	4	Модель возможного нарушителя и угроз безопасности	2	
	5	Меры по защите информации в рамках построения КСЗИ	2	
	6	Особенности защиты информации в кабинете руководителя предприятия	2	
Тема 1.12. Сущность и содержание контроля функционирования комплексной системы защиты информации предприятия	**Содержание учебного материала.**		**4**	1-2
	1	**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	
	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	
	Практические занятия.		**4**	2
	1	Основные задачи контроля функционирования КСЗИ	2	
	2	Анализ и использование результатов проведения контрольных мероприятий в области защиты информации	2	
Тема 1.13. Управление комплексной системой защиты	**Содержание учебного материала.**		**8**	1-2
	1	**Понятие и основные виды чрезвычайных ситуаций в организации.**	2	

информации в условиях чрезвычайных ситуаций	2	**Технология принятия решений в условиях чрезвычайных ситуаций**	2	
	3	**Факторы, влияющие на принятие решений в условиях чрезвычайных ситуаций.** Неопределенность. Ограниченность во времени. Физио-психологическое состояние лиц, принимающих решения и их исполнителей	2	
	4	**Подготовка мероприятий на случай возникновения чрезвычайных ситуаций.**	2	
	Практические занятия.		**2**	2
	1	Практические действий работников при чрезвычайных ситуациях.	2	
Тема 1.14. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации организации	**Содержание учебного материала.**		**2**	
	1	**Вероятностный подход. Оценочный подход.**	2	1-2
	Практические занятия.		**4**	2
	1	Определение требований к средствам вычислительной техники (СВТ).	2	
	2	Определение требований к автоматизированным системам (АС).		
Тема 1.15. Методы и модели оценки эффективности комплексной системы защиты информации	**Содержание учебного материала.**		**4**	1-2
	1	**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	
	2	**Экономический подход к оценке эффективности КСЗИ.** Определение размеров ущерба с использованием моделей «осведомленность — эффективность. Определение размеров ущерба с использованием экспертных оценок.	2	1-2
	Практические занятия.		**4**	3
	1	Методы проведения экспертного опроса	2	
	2	Определение затрат на защиту информации.	2	
	Консультации по курсовому проекту.		**10**	
Самостоятельная работа обучающихся по разделу 1.			**84**	
1. Понятия безопасности и защищенности (презентация). 2. Служебная и коммерческая тайны - сравнительная характеристика (презентация). 3. Основные требования ФСТЭК России по защите персональных данных (презентация). 4. Подходы зарубежных стран к защите конфиденциальной информации (доклад). 9. Порядок разработки Перечня сведений, составляющих коммерческую тайну, внесение в него изменений и дополнений (презентация). 10. Основные источники защищаемой информации (презентация). 11. Интеллектуальная собственность предприятия как объект защиты (презентация). 12. Необходимость защиты «ноу-хау» (презентация).				

13. Категории доступа помещений предприятия для работы с защищаемой информацией (презентация). 14. Объективные и субъективные факторы, создающие угрозу информационной безопасности (презентация). 15. Описание каналов утечки информации (презентация) 16. Задачи КСЗИ по выявлению угроз и каналов утечки информации (презентация). 17. Классификация методов и средств защиты данных (презентация). 18. Общее содержание работ по организации КСЗИ (презентация). 19. Основные направления развития и совершенствования МТО ЗИ (презентация). 20. Перечень основных внутренних организационно-распорядительных документов по организации защиты персональных данных организации (презентация). 21. Анализ технических средств охраны для оборудования режимных помещений (презентация). 22. Анализ технических средств и систем контроля доступа на режимные территории (презентация). 23. Принципы управления КСЗИ: комплексность, своевременность, непрерывность, активность, законность, обоснованность, специализация, взаимодействие и координация, централизация управления (сравнительный анализ). 24. Основные методы контроля, виды контроля эффективности защиты (реферат). 25. Определение упущенной выгоды в результате ограничений на распространение информации (реферат). 26. Требования основных нормативно-методических документов ФСТЭК России (СТР-К, ГОСТ) в области информационной безопасности (презентационные доклады).				
Дифференцированный зачет			**2**	
Раздел 2. Работа подразделений защиты информации.				
МДК.01.02. Организация работ подразделений защиты информации.				
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. Рекомендуемые учебные пособия.		**2**	1
Тема 2.1. Место и роль подразделений защиты информации в системе защиты информации.	**Содержание учебного материала.**		**10**	1-2
	1	Назначение подразделений защиты информации.	2	
	2	Место подразделений защиты информации в системе безопасности предприятия.	2	
	3	Подразделения защиты информации как составная часть системы защиты.	2	
	4	Подразделения защиты информации как орган управления защитой информации	2	
	5	Подразделения защиты информации как координатор деятельности по обеспечению безопасности информации.	2	
	Практические занятия.		**2**	2
	1	Служба защиты информации как координатор деятельности по обеспечению безопасности информации	2	
Тема 2.2. Задачи и функции подразделений защиты	**Содержание учебного материала.**		**2**	1-2
	1	Организационные. Технологтческие и координационные задачи и функции	2	

информации.		подразделений зашиты информации.		
	Практические занятия.		**4**	2
	1	Взаимосвязь и соотношение организационных, технологических и координационных задач и функций.	2	
	2	Факторы, влияющие на определение задач и функций службы защиты информации.	2	
Тема 2.3. Структура и штаты подразделений защиты информации.	**Содержание учебного материала.**		**8**	1-2
	1	Общая структурная схема подразделений защиты информации.	2	
	2	Виды и типы организационных структур подразделений защиты информации.	2	
	3	Централизованная и децентрализованная структуры подразделений защиты информации, условия, критерии, определяющие выбор структур.	2	
	4	Должностной состав сотрудников подразделений защиты информации, его зависимость от характера выполняемых работ.	2	
	Практические занятия.		**8**	2
	1	Факторы, определяющие конкретную структуру подразделений защиты информации.	2	
	2	Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений защиты информации.	2	
	3	Функции сотрудников и уполномоченных подразделений защиты информации	2	
	4	Факторы, определяющие численность сотрудников подразделений защиты информации.	2	
Тема 2.4.Организационные основы и принципы деятельности подразделений защиты информации.	**Содержание учебного материала.**		**8**	1-2
	1	Порядок создания подразделений защиты информации.	2	
	2	Структура и содержание положения о подразделениях защиты информации.	2	
	3	Состав и содержание других нормативных документов, регламентирующих деятельность подразделений защиты информации.	2	
	4	Основные принципы организации и деятельности подразделений защиты информации.	2	
	Практические занятия.		**6**	2-3
	1	Условия и факторы, влияющие на организацию работы подразделений защиты информации.	2	
	2	Порядок взаимодействия подразделений защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации.	2	
	3	Организация взаимодействия службы защиты информации и подразделений предприятия.	2	
Тема 2.5. Подбор, расстановка и обучение сотрудников подразделений защиты информации.	**Содержание учебного материала.**		**6**	1-2
	1	Общие требования, предъявляемые к сотрудникам подразделений защиты информации.	2	
	2	Формы создания и способы поддержания необходимого микроклимата в коллективе.	2	

	3	Формы повышения квалификации сотрудников.	2	
	Практические занятия.		**6**	2
	1	Особенности подбора кадров.	2	
	2	Методы получения информации о кандидатурах на должности.	2	
	3	Социально-психологические факторы, влияющие на расстановку кадров.	2	
Тема 2.6. Организация труда сотрудников подразделений защиты информации.	**Содержание учебного материала.**		**12**	1-2
	1	Деятельность сотрудников подразделений защиты информации.	2	
	2	Структура и содержание должностных инструкций сотрудников подразделений защиты информации.	2	
	3	Организация рабочих мест сотрудников подразделений зашиты информации.	2	
	4	Оснащение оборудованием, техническими средствами рабочих мест сотрудников подразделений зашиты информации.	2	
	5	Обеспечение необходимых условий труда. Охрана труда.	2	
	6	Карты организации трудового процесса.	2	
	Практические занятия.		**6**	2
	1	Обеспечение персональной ответственности за сохранность носителей информации.	2	
	2	Специфика деятельности сотрудников службы защиты информации.	2	
	3	Распределение обязанностей между сотрудниками подразделений защиты информации.	2	
Тема 2.7. Принципы и методы управления подразделений защиты информации.	**Содержание учебного материала.**		**16**	1-2
	1	Принципы управления подразделениями защиты информации.	2	
	2	Понятие и сущность методов управления.	2	
	3	Система методов управления.	2	
	4	Административно-правовые методы управления.	2	
	5	Экономические методы управления.	2	
	6	Социально-психологические методы управления.	2	
	7	Взаимосвязь методов управления.	2	
	8	Необходимость комплексного и системного применения методов управления службой защиты информации.	2	
	Практические занятия.		**16**	2-3
	1	Проектирование структуры службы защиты защиты информации.	2	
	2	Организационные основы и принципы деятельности службы защиты информации. Пакет документов.	2	
	3	Организационные основы и принципы деятельности службы защиты информации.	2	
	4	Система конфиденциальной информации фирмы.	2	
	5	Организация информационно-аналитической работы.	2	
	6	Оценка удовлетворѐнности потребностей работника методом парных сравнений.	2	

	7	Оплата и стимулирование труда.	2	
	8	Кадровое обеспечение службы ИБ.	2	
Тема 2.8. Технология управления подразделениями защиты информации.	**Содержание учебного материала.**		**20**	1-2
	1	Состав управленческих функций.	2	
	2	Содержание управленческих функций.	2	
	3	Технология управления подразделениями защиты информации.	2	
	4	Значение управленческих решений.	2	
	5	Цели планирования.	2	
	6	Виды планирования, их назначение.	2	
	7	Содержание и структура планов.	2	
	8	Технология планирования.	2	
	9	Методы и формы контроля выполнения планов	2	
	10	Критерии эффективности подразделений защиты информации.	2	
	Практические занятия.		**26**	2-3
	1	Методы оценки качества подразделений защиты информации.	2	
	2	Пути повышения эффективности управления подразделениями защиты информации.	2	
	3	Способы повышения эффективности управления подразделением защиты информации.	2	
	4	Критерии эффективности службы защиты информации	2	
	5	Методы оценки качества службы защиты информации.	2	
	6	Пути и способы повышения эффективности управления службой защиты информации.	2	
	7	Статус подразделения защиты информации в структуре предприятия.	2	
	8	Организационные, технологические и координационные задачи и функции.	2	
	9	Виды организационных структур подразделений защиты информации.	2	
	10	Условия и факторы, влияющие на организацию работы подразделений защиты информации.	2	
	11	Специфические требования, предъявляемые к сотрудникам службы защиты информации.	2	
	12	Методика определения численного состава подразделений защиты информации.	2	
	13	Особенности приема сотрудников в подразделения защиты информации.	2	
	Консультации по курсовому проекту.		**10**	
Самостоятельная работа обучающихся по разделу 2			**84**	
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.				
Раздел 3. Работа персонала с конфиденциальной информацией.			**252**	
МДК.01.03. Организация работы персонала с конфиденциальной информацией.			**252**	
Введение	1	Предмет, цели, задачи и содержание междисциплинарного курса Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.	**2**	1
Тема 3.1. Общая характеристика нормативно-правовой базы	**Содержание учебного материала.**		**14**	1-2
	1	Понятие и особенности конфиденциальной информации	2	
	2	Персональные данные	2	
	3	Тайна следствия и судопроизводства	2	
	4	Служебная тайна	2	
	5	Профессиональная тайна	2	
	6	Коммерческая тайна	2	
	7	Секрет производства и служебный секрет производств	2	
	Практические занятия.		**4**	2
	1	Обработка персональных данных без использования средств информатизации	2	
	2	Нормативно-правовая база организации работы с конфиденциальными документами	2	
Тема 3.2 Документирование конфиденциальной информации	**Содержание учебного материала.**		**14**	1-2
	1	Особенности документирования конфиденциальной информации	2	
	2	Определение степени ограничения доступа к документам и использование отметки конфиденциальности при оформлении документов	2	
	3	Разработка перечня конфиденциальной документированной информации	2	
	4	Учет бумажных носителей конфиденциальной информации	2	
	5	Учет проектов конфиденциальной документированной информации	2	

	6	Особенности создания и изготовления конфиденциальных документов с помощью средств ЭВТ, их печатания, тиражирования, размножения	2	
	7	Учет использования и хранения печатей, штампов, бланков, необходимых для оформления конфиденциальных документов	2	
	Практические занятия.		**10**	2
	1	Разработка перечня документированной конфиденциальной информации	2	
	2	Определение степени разграничения доступа к документам и использование отметки конфиденциальности при оформлении документов	2	
	3	Обработка поступающих и внутренних конфиденциальных документов, их учет и регистрация	2	
	4	Учет и регистрация внутренних конфиденциальных документов	2	
	5	Исполнение и контроль за исполнением конфиденциальных документов	2	
Тема 3.3. Организация конфиденциального документооборота	**Содержание учебного материала.**		**14**	1-2
	1	Особенности учета и регистрации конфиденциальной документированной информации	2	
	2	Обработка поступающих конфиденциальных документов, их учет и регистрация		
	3	Учет и регистрация внутренних (созданных/изданных) конфиденциальных документов	2	
	4	Технологии исполнения и контроля за исполнением конфиденциальных документов	2	
	5	Учет и регистрация отправляемых (исходящих) конфиденциальных документов, их экспедиционная обработка и рассылка	2	
	6	Учет конфиденциальной документированной информации инвентарного (выделенного) хранения	2	
	7	Учет конфиденциальной информации при ее автоматизированной обработке	2	
	Практические занятия.		**12**	2-3
	1	Документальный фонд организации	2	
	2	Формирование конфиденциальных дел	2	
	3	Оформление конфиденциальных дел	2	
	4	Экспертиза ценности конфиденциальных документов	2	
	5	Подготовка конфиденциальных документов и дел для архивного хранения	2	
	6	Подготовка конфиденциальных документов и дел к уничтожению	2	
Тема 3.4. Разрешительная система доступа к конфиденциальной информации	**Содержание учебного материала.**		**14**	1-2
	1	Основные требования к разрешительной системе доступа	2	
	2	Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет	2	

		производства и служебный секрет производства		
	3	Особенности доступа к конфиденциальной документированной информации при ее предоставлении уполномоченным органам государственной власти	2	
	4	Особенности доступа к конфиденциальной документированной информации, составляющей персональные данные	2	
	5	Особенности доступа к архивным конфиденциальным документам	2	
	6	Особенности доступа должностных лиц при их командировании к конфиденциальной документированной информации	2	
	7	Учет персонала, получившего доступ к конфиденциальной документированной информации, и (или) лиц, которым она была передана или предоставлена	2	
	Практические занятия.		**14**	2
	1	Основные требования к разрешительной системе доступа	2	
	2	Особенности доступа к конфиденциальной документированной информации	2	
	3	Доступ к конфиденциальной информации, предоставленной органами государственной власти	2	
	4	Доступ к конфиденциальной документированной информации, составляющей ПД	2	
	5	Доступ к архивным конфиденциальным документам	2	
	6	Доступ должностных лиц при их командировании к конфиденциальной информации	2	
	7	Учет персонала, получающего доступ к конфиденциальной информации	2	
Тема 3.5. Режим конфиденциальности документированной информации	**Содержание учебного материала.**		**8**	1-2
	1	Режим обмена конфиденциальной документированной информацией	2	
	2	Режим сохранности конфиденциальных документов и дел	2	
	3	Режим конфиденциальности при проведении совещаний и переговоров	2	
	4	Проверка наличия носителей конфиденциальной информации	2	
	Практические занятия		**6**	2
	1	Подбор персонала на должности, связанные с работой с конфиденциальной информацией	2	
	2	Допуск к секретной информации	2	
	3	Организация работы с персоналом, имеющим доступ к конфиденциальной информацией	2	
Тема 3.6. Система защищенного электронного документооборота	**Содержание учебного материала.**		**16**	1-2
	1	Особенности конфиденциального электронного документооборота	2	
	2	Основные виды угроз информационной безопасности организации	2	
	3	Основные требования и меры по защите конфиденциальной информации,	2	

		циркулирующей в эксплуатируемой автоматизированной информационной системе		
	4	Организация работ при создании системы защиты электронного документооборота	2	
	5	Организация проведения работ по защите конфиденциальной информации при ее автоматизированной обработке	2	
	6	Обеспечение контроля защиты электронного документооборота	2	
	7	Аттестация автоматизированных информационных систем по требованиям безопасности информации	2	
	8	Защита от вредоносных программ. Защита системы электронных сообщений.	2	
	Практические занятия.		**28**	2-3
	1	Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия	2	
	2	Порядок назначения комиссии для аттестации помещений на пригодность их для ведения конфиденциальных работ	2	
	3	Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных изделий и документов	2	
	4	Организация подготовки и проведения совещаний и переговоров	2	
	5	Организационные мероприятия при проведении совещаний и переговоров	2	
	6	Технические мероприятия при проведении совещаний и переговоров	2	
	7	Способы предотвращения подслушивания и наблюдения при проведении совещаний и переговоров	2	
	8	Организация защиты информации при приеме в организации посетителей и командированных лиц	2	
	9	Организация защиты информации при приеме в организации иностранных представителей	2	
	10	Организация защиты информации при осуществлении рекламной и публикаторской деятельности		
	11	Организация защиты информации при подготовке материалов к открытому опубликованию	2	
	12	Аналитическая работа как основа управления системой организационной защиты информации	2	
	13	Планирование процессов организационной защиты информации	2	
	14	Контроль функционирования системы организационной защиты информации	2	
	Консультации по курсовому проекту.		**10**	
Самостоятельная работа обучающихся по разделу 3.			**84**	
1. Законы РФ «О коммерческой тайне», «Об информации, информатизации и защите информации», «О персональных данных»				

2. Нормативно-методическая база организации работы с документами, содержащими служебную тайну 3. Сущность и принципы ограничения доступа к информации и документам 4. Нормативно-правовые основы организации работы с документами, содержащими коммерческую тайну 5. Создание и изготовление конфиденциальных документов с помощью ЭВМ их печатания, тиражирования и размножения. 6. Учет использования и хранения печатей, штампов, бланков, необходимых для оформления документов 7. Понятие "внутри 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. 9. Экспедиционные технологии обработки и учета поступающих пакетов с конфиденциальной информацией 10. Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта. 11. Порядок допуска работников в помещения, где ведутся конфиденциальные работы. 12. Организация работы по защите информации при осуществлении публицистической деятельности и связей с прессой; участие в ней Службы безопасности 13. Организация контроля за выполнением распорядка дня лицами, работающими на режимных объектах. 14. Создание отдельных (выделенных) производственных зон (зон доступа) по типу и степени конфиденциальности работ с самостоятельными системами организации и контроля доступа. 15. Методика проектирования системы пропускного и внутри объектового режимов и оценки эффективности их функционирования. 16. Методы оценки эффективности защитных мероприятий в рекламной и публицистической деятельности. 17. Виды и способы охраны. Понятие о рубежах охраны. Многорубежная система охраны 18. Порядок вывоза (выноса) материальных ценностей и документации с территории организации и ввоза (вноса) их на территорию 19. Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта. Порядок допуска работников в помещения, где ведутся конфиденциальные работы 20. Методика проектирования системы пропускного и внутри объектового режимов и оценки эффективности их функционирования 21. Составление списков участников совещания. Определение состава информации, используемой в ходе совещаний, переговоров		
Дифференцированный зачет.	**2**	
Учебная практика:	**108**	
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; 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; 18. Дифференцированный зачёт.		
Производственная практика:	**108**	
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 рабочих совещаний; 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, 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. 18. Дифференцированный зачёт.		

Для характеристики уровня освоения учебного материала используются следующие обозначения:

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

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

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

Тема курсовой работы: Подготовка объектов информатизации предприятия к аттестации по требованиям защиты конфиденциальной информации» (объекты согласно утвержденного перечня).

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие кабинета общепрофессиональных дисциплин и профессиональных модулей по направлению Информационная безопасность, лаборатории программно-аппаратных и технических средств защиты информации, электронного документооборота, лаборатории компьютерной техники.

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 программно-аппаратных и технических средств защиты информации электронного документооборота.

- 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 компьютерной техники:

- 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

Основные источники

1. Нестеров С.П. Информационная безопасность: Ученик и практикум для СПО. – М.: Юрвайт, 2019. Электронный ресурс: ЭБС Юрайт https://biblio-online.ru/viewer/informacionnaya-bezopasnost-442312#page/1

2. Мельников В.П., Клеймёнов С.А., Петраков А.М. Информационная безопасность: Учеб. пос. Для СПО.- 8-е изд., испр. – М.: Академия, 2013.

3. Куняев Н.Н. и др. Конфиденциальное делопроизводство и защищённый электронный документооборот: Учебник для ВУЗов. – М.: ЛОГОС, 2014.

4. Полякова Т.А. Организационное и правовое обеспечение информационной безопасности: Учебник и практикум для СПО / Отв. ред., Стрельцов А.А. – Юрайт, 2016.

5. Внуков А. А. Основы информационной безопасности. Защита информации: Учеб. пос. для СПО. – 2-е изд., испр. и доп. - М.: Юрайт, 2019. - Электронный ресурс: ЭБС Юрайт. https://biblio-online.ru/viewer/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-431332#page/1

Рекомендуемые источники:

1. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г.А. Бузов. - М.: Горячая линия-Телеком, 2010.

2. Голицына, О.Л. Информационные технологии: учебник для учрежд. сред. проф. образ. – 2-е изд., перераб. и доп./ О.Л. Голицына, Н.В. Максимов, Т.Л. Партыка, И.И. Попов. – М.: ФОРУМ-ИНФРА-М, 2008. – [Рекомендовано МО РФ].

3. Киселев, С.В. Основы сетевых технологий: учеб. пособие для нач. проф. образования / С.В. Киселев, И.Л. Киселев. – М.: Академия, 2008. – (Непрерывное профессиональное образование).
4. Маркеев А.И. Правовая защита информации: учеб. пособие / А.И. Маркеев. Новосибирск: СГГА, 2011
5. Михайлов А.В. Компьютерные вирусы и борьба с ними / А.В. Михайлов . - М.: Диалог-МИФИ, 2011
6. Кузин, А. В. Компьютерные сети: учеб. пособие / А.В. Кузин, В.М. Демин. – М.: Форум, 2008.
7. Петренко С.А. Политики информационной безопасности / С.А. Петренко, В. А. Курбатов. - М.: Академия АйТи, 2011

Интернет ресурсы:

1. Бесплатный для студентов, аспирантов, школьников и преподавателей доступ к полным лицензионным версиям инструментов Microsoft для разработки и дизайна - http://www.dreamspark.ru/
2. Интернет-Университет Информационных технологий http://www.intuit.ru/
3. Закон «Об информации, информационных технологиях и о защите информации» ФЗ N 149-ФЗ от 27 июля 2006 года [Электронный ресурс]/ http://www.rg.ru/ Режим доступа:http://www.rg.ru/2006/07/29/informacia-dok.html.

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 и профессиональные модули, изучение которых предшествует освоению данного профессионального модуля:

дисциплины:

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 экзамена (МДК.01.02) и дифференцированного зачета (МДК.01.01 и МДК.01.03). 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 работа (проект).

При работе над курсовыми работами (проектами) 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 (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): наличие высшего профессионального образования, соответствующего профилю модуля **Участие в планировании и организации работ по обеспечению защиты объекта** и специальности **10.02.01 Организация и технология защиты информации.**

Педагогические кадры, обеспечивающие обучение по данному профессиональному модулю должны иметь высшее образование, соответствующее профилю профессионального

модуля, и проходить повышение квалификации и (или) стажировку в профильных организациях не реже одного раза в три года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой

Инженерно-педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин: Технические средства информатизации, Базы данных и Основы информационной безопасности.

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 сбора и обработки материалов; - эффективное использование средств обнаружения возможных каналов утечки конфиденциальной информации.	Экспертная оценка выполненной работы. Текущий контроль в форме: - защиты практических работ; - контрольных работ по темам МДК. - наблюдение за выполнением практических работ. Зачеты по производственной практике и по каждому из разделов профессионального модуля. Зачеты и экзамены по МДК. Защита курсового проекта. Комплексный экзамен по профессиональному модулю.
ПК1.2 Участвовать в разработке программ и методик организации защиты информации на объекте.	- правильность использования методик 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	-грамотное ведение учета, обработки, хранения, передачи, использования различных	

носителей конфиденциальной информации.	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 объектов информатизации, подлежащих защите.
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.

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

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Принимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности	демонстрация интереса к будущей профессии;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
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;	
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	решение стандартных и нестандартных профессиональных задач в области защиты информации;	
Осуществлять поиск и использование информации, необходимые для эффективного	эффективный поиск необходимой информации, использование различных источников, включая	

выполнения профессиональных задач, профессионального и личностного развития	электронные;	
Использовать информационно-коммуникационные технологии в профессиональной деятельности	работа с прикладными программами в области защиты информации;	
Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями	взаимодействие с обучающимися и преподавателями в ходе обучения;	
Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	самоанализ и коррекция результатов собственной работы;	
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	организация самостоятельных занятий при изучении профессионального модуля;	
Ориентироваться в условиях частой смены технологий профессиональной деятельности	анализ инноваций в области защиты информации	
Применять математический аппарат для решения профессиональных задач	применение математического анализа для решения профессиональных задач	
Оценивать значимость документов, применяемых в профессиональной деятельности	самостоятельная оценка значимости документов, применяемых в профессиональной деятельности	
Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность	анализ структуры федеральных органов исполнительной власти, обеспечивающих информационную безопасность	