ГОСУДАСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«НИЖЕГОРОДСКИЙ ПРОМЫШЛЕННО- ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ 01. УЧАСТИЕ В ПЛАНИРОВАНИИ И ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОБЪЕКТА

10.02.01 ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Нижний Новгород
2021 г.

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

Организация-разработчик:
ГБПОУ «Нижегородский промышленно- технологический техникум»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения программы

Рабочая программа профессионального модуля (далее программа) является частью программы подготовки квалифицированных рабочих, служащих в соответствии с ФГОС СПО по специальности: специальности среднего профессионального образования 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.

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

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями студент 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

1.3. Количество часов на освоение программы профессионального модуля:

Максимальной учебной нагрузки обучающихся – **501** час, в том числе:

практической работы – **130** часов;

самостоятельной работы обучающихся – **167** часов;

учебной и производственной практики – **180** часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение студентами видом профессиональной деятельности Организация и технология защиты информации, 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.

Личностные результаты реализации программы воспитания *(дескрипторы)*	**Код личностных результатов реализации программы воспитания**
Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации	**ЛР 13**
Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм	**ЛР 14**
Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.	**ЛР 15**

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОАНЛЬНОГО МОДУЛЯ

3. 1. Тематический план профессионального модуля ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта

Код профес-сиональных компетенций	Наименование разделов профессионального модуля	Всего часов	Объем времени, отведенный на основание междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка студентов			Самостоятельная работа студентов		Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	в т.ч. лаборторные 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.	**МДК 01.01.** Обеспечение организации системы безопасности предприятия.	**201**	**134**	40	30	**64**	-	-	-
ПК 1.1. – 1.9.	**МДК 01.02.** Организация работ подразделений защиты информации.	**150**	**100**	50	-	**50**	-	-	-
ПК 1.1. – 1.9.	**МДК 01.03.** Организация работы персонала с конфиденциальной информацией.	**150**	**100**	40	-	**60**	-	-	-
ПК 1.1. – 1.9.	Учебная практика							**72**	
ПК 1.1. – 1.9.	Производственная практика (по профилю специальности)							-	**108**
	Всего:	**501**	**334**	**130**	**30**	**174**	-	**72**	**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 работ (проект)		Объем часов	Код ЛР, ОК, ПК
1	2		3	4
Раздел 1. Участие в планировании работ по обеспечению защиты объекта			**201**	ЛР 13-15, ОК 1 - 12 ПК 1.1 - 1.9
МДК 01.01. Обеспечение организации системы безопасности предприятия			**201**	
Тема 1. Общие положения концепции обеспечения безопасности информации в системе организации.	**Содержание**		**2**	
	1.	Назначение и правовая основа обеспечения безопасности информации в системе организации.	2	
Тема 2. Объекты защиты	**Содержание**		**8**	
	1.	Объекты информационной безопасности.	2	
	2.	Назначение, цели создания и эксплуатации автоматизированной системы (АС) организации как объекта информатизации. Структура, состав и размещение основных элементов АС организации.	2	
	4.	Категории информационных ресурсов, подлежащих защите. Категории пользователей АС организации.	2	
	6.	Уязвимость основных компонентов АС организации	2	
Тема 3. Цели и задачи обеспечения безопасности информации.	**Содержание**		**10**	
	1.	Интересы затрагиваемых при эксплуатации АС организации субъектов информационных отношений.	2	
	3.	Цели и организация защиты от вмешательства в процесс функционирования АС организации.	2	
	4.	Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам. Регистрация действия пользователей при использовании защищаемых ресурсов.	2	
	6.	Организация защиты от несанкционированной модификации, контроль целостности. Своевременное выявление источников угроз безопасности информации.	2	
	8.	Основные пути достижения целей защиты. Решение задач системы защиты.	2	
Тема 4. Основные непреднамеренные угрозы	**Содержание**		**2**	
	1.	Угрозы безопасности информации и их источники. Пути реализации непреднамеренных искусственных угроз.	2	

безопасности информации АС организации.	**Практические занятия**		**14**	
	1.	Меры по нейтрализации действий сотрудников организации, приводящие к частичному или полному отказу системы.		
	2.	Защита от несанкционированного запуска технологических программ.		
	3.	Защита от несанкционированного внедрения и использования неучтенных программ.		
	4.	Защита от непреднамеренного заражения компьютера вирусами.		
	5.	Защита от разглашения, передачи, утраты атрибутов разграничения доступа.		
	6.	Защита от игнорирования организационных ограничений.		
	7.	Защита от некомпетентного использования настроек, неправомерного отключения средств защиты. от ввода ошибочных данных.		
Тема 5. Основные умышленные угрозы безопасности информации.	**Содержание**		**10**	
	1.	Умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала. Утечка информации по техническим калам.	2	
	3.	Перехват информации ограниченного распространения.	2	
	4.	Неформальная модель возможных нарушителей.	2	
	5.	Типы нарушителей в информационной системе организации. Внутренние и внешние нарушители.	2	
	6.	Ограничения и предположения о характере действия возможных нарушителе.	2	
	Практические занятия		**14**	
	1.	Организация мер по нейтрализации физического разрушения компонентов АС.		
	2.	Организационные меры по нейтрализации внедрения агентов в число персонала системы, имеющих доступ.		
	3.	Нейтрализация несанкционированного копирования информации.		
	4.	Нейтрализация незаконного получения паролей и других реквизитов разграничения доступа.		
	5.	Нейтрализация несанкционированного использования АРМ пользователей.		
	6.	Защита от перехвата данных, передаваемых по каналам связи.		
	7.	Защита от вмешательства в процесс функционирования АС сетей общего пользования.		
Тема 6. Основные положения технической политики в области обеспечения безопасности информации АС	**Содержание**		**18**	
	1.	Техническая политика в области обеспечения безопасности информации. Основные направления реализации технической политики обеспечения	2	
	3.	Системы допуска исполнителей. Инженерно-технические и организационные меры охраны.	2	

организации.	5.	Формирование режима безопасности информации. Комплекс мер по формированию режима безопасности информации.	2	
	7.	Организационно-правовой режим. Приказы и распоряжения по установлению режима безопасности информации. Инструкции и функциональные обязанности сотрудников.	2	
	10.	Организационно-технические мероприятия по защите информации.	2	
	11.	Физическая охрана объектов информатизации.	2	
	12.	Выполнение режимных требований при работе с информацией.	2	
	13.	Мероприятия технического контроля.	2	
	14.	Оснащение техническими средствами хранения и обработки информации.	2	
	Практические занятия		**12**	
	1.	Разработка организационно-распорядительных документов для установления режима безопасности информации.		
	2.	Разработка комплекса мер для установления режима безопасности информации.		
	3.	Разработка инструкций и функциональных обязанностей сотрудников отвечающих режиму безопасности информации.		
	4.	Разграничение допуска к информационным ресурсам.		
	5.	Организация технического контроля.		
	6.	Разработка комплекса мер, позволяющих выявлять каналы утечки информации.		
Тема 7. Основные принципы построения системы комплексной защиты информации.	**Содержание**		**14**	
	1.	Принципы построения системы комплексной защиты информации.	2	
	2.	Принцип законности и системности.	2	
	3.	Принципы комплексности и непрерывности защиты.	2	
	4.	Принципы преемственности, совершенствования и разумной достаточности.	2	
	5.	Принцип персональной ответственности.	2	
	6.	Принцип научной обоснованности и технической реализуемости.	2	
	7.	Принцип обязательности контроля.	2	
Курсовая работа			**30**	
Самостоятельная работа при изучении раздела 1. Систематическая проработка конспектов занятий, учебной и специальной литературы по страховой тематике (по вопросам параграфам, главам учебных пособий, составленных преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите. Проработка нормативно-правовой базы и инструктивного материала по темам раздела. Основные компоненты компьютерных сетей.			**67**	

Основные виды потенциальных опасностей и их последствия в страховой деятельности и быту, принципы снижения вероятности их реализации.				
Примерная тематика внеаудиторной самостоятельной работы: Разработка схем-конспектов для систематизации закрепления учебного материала. Подготовка сообщений и рефератов по темам раздела.				
Раздел 2. Работа подразделений защиты информации.			**150**	ЛР 13-15, ОК 1 - 12 ПК 1.1 - 1.9
МДК 01.02 Организация работ подразделений защиты информации			**150**	
Тема 1. Общие **положения** подразделения по защите информации (ЗИ).	**Содержание**		**2**	
	1.	Руководство подразделений по ЗИ. Цели создания подразделения по ЗИ. Принципы организации подразделения по ЗИ.	2	
	Практические занятия		**10**	
	1	Анализ состояния информационной безопасности в организации.	4	
	2	Решение о необходимости создания структурного подразделения по ЗИ.	4	
	3.	Разработка проекта структуры подразделения ЗИ.	2	
Тема 2. Структура подразделения по ЗИ.	**Содержание**		**10**	
	1.	Состав и штатная численность подразделения по ЗИ.	2	
	2.	Обязанности специалиста подразделения по ЗИ.	2	
	3.	Основные этапы построения подразделения по ЗИ.	2	
	4.	Типовая структура подразделения по ЗИ.	2	
	5.	Требования к уровню подготовки руководителя подразделения по ЗИ.	2	
	Практические занятия		**2**	
	6.	Организация руководства подразделения по ЗИ.	2	
Тема 3. Основные задачи подразделений по ЗИ.	**Практические занятия**		**12**	
	1.	Разработка единой политики (концепции) обеспечения информационной безопасности организации.	4	
	2.	Организация мероприятий и координация работ всех подразделений по ЗИ.	4	
	3.	Контроль и оценка эффективности принятых мер и применяемых средств защиты информации.	4	
Тема 4. Функции подразделений по ЗИ.	**Содержание**		**4**	
	1	Кадровая работа подразделений по ЗИ.	2	
	2	Обеспечение сотрудников фирмы информационной поддержкой по вопросам ИБ.	2	

	Практические занятия		**24**	
	1	Разработка концепции и политики информационной безопасности организации.	4	
	2	Выработка принципов классификации информационных активов организации и оценки их защищенности.	4	
	3	Оценка и управление информационными рисками.	4	
	4	Обучение сотрудников организации по вопросам обеспечения ИБ.	4	
	5	Согласование частной политики и отдельных регламентов безопасности среди подразделений организации.	4	
	6	Подготовка аналитических справок о текущем состоянии информационной безопасности.	4	
Тема 5. Регламентирующие документы подразделения по ЗИ. .	**Содержание**		**4**	
	1.	Внутренние регламентирующие документы подразделения по ЗИ.	2	
	2.	Внешние регламентирующие документы подразделения по ЗИ.	2	
Тема 6. Взаимоотношения порразделения по ЗИ с другими подразделениями.	**Содержание**		**10**	
	1.	Работа с отделом кадров.	2	
	2.	Работа с отделом по организации и оплаты труда.	2	
	3.	Работа с отделом подготовки кадров.	2	
	4.	Работа с юридическим отделом.	2	
	5.	Организация работы подразделения со всеми производственными и технологическими подразделениями.	2	
Тема 7. Права подразделения по ЗИ.	**Содержание**		**10**	
	1.	Допуск к работе основных структурных подразделений.	4	
	2.	Порядок получения лицензии на выполнение работ по ЗИ.	2	
	3.	Финансирование подразделения по ЗИ.	2	
	4.	Ответственность отдела по ЗИ.	2	
	Практические занятия		**2**	
	1	Контроль за деятельностью структурных подразделений предприятия.	2	
Тема 8. Нормативно-методические основы деятельности подразделения по ЗИ.	**Содержание**		**10**	
	1.	Основные нормативные документы, регулирующие деятельность подразделения по ЗИ.	2	
	2.	Должностные инструкции сотрудников подразделения.	2	
	3.	Положение о сохранении конфиденциальной информации организации.	2	

	4.	Инструкция о допуске и доступе к конфиденциальной информации и правила обращения с ней.	2	
	5.	Соглашение о неразглашении сведений конфиденциального характера организации.	2	
Самостоятельная работа при изучении раздела 2			**50**	
Систематическая проработка конспектов занятий, учебной и специальной литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите.				
Тематика внеаудиторной самостоятельной работы Изучение нормативных документов. Рефераты по темам раздела. Оформление пакета документов, связанных с работой подразделения по ЗИ.				
Раздел 3. Работа персонала с конфиденциальной информацией.			**150**	ЛР 13-15, ОК 1 - 12 ПК 1.1 - 1.9
МДК 01.03 Организация работы персонала с конфиденциальной информацией.			**150**	
Тема 1. Особенности работы с конфиденциальной информацией.	**Содержание**		**6**	
	1.	Общие положение. Конфиденциальная информация.	2	
	2.	Нормативная база конфиденциального делопроизводства.	2	
	3.	Особенности работы с конфиденциальной информацией	2	
	Практические занятия		**4**	
	1.	Обработка персональных данных без использования средств автоматизации.	4	
Тема 2. Документирование конфиденциальной информации.	**Содержание**		**6**	
	1.	Особенности документирования конфиденциальной информации.	2	
	2.	Учет бумажных носителей конфиденциальной информации и их проектов.	2	
	3.	Документирование конфиденциальной информации	2	
	Практические занятия		**12**	
	1.	Разработка перечня конфиденциальной документированной информации.	4	
	2.	Определение степени ограничения доступа к документам.	4	
	3.	Использование отметки конфиденциальности при оформлении документов.	4	
Тема 3. Организация конфиденциального документооборота.	**Содержание**		**10**	
	1	Учет и регистрация входящих конфиденциальных документов.	2	
	2	Учет и регистрация внутренних конфиденциальных документов.	2	
	3	Реестр конфиденциальной информации. Ведение реестра конфиденциальной информации.	2	

	4	Организация конфиденциального документооборота. Обработка поступающих и внутренних конфиденциальных документов	2	
	5	Исполнение и контроль за исполнением конфиденциальных документов	2	
	Практические занятия		**4**	
	1.	Обработка поступающих и внутренних конфиденциальных документов.	2	
	2.	Учет и регистрация внутренних конфиденциальных документов.	2	
Тема 4. Разрешительная система доступа к конфиденциальной информации.	**Содержание**		**10**	
	1.	Регламент доступа к конфиденциальной информации.	2	
	2.	Обязательство о неразглашении конфиденциальной информации.	2	
	3.	Федеральный закон №152 "О персональных данных"	2	
	4.	Доступ к архивным конфиденциальным документам	2	
	5.	Органы государственной власти. Служебная и коммерческая тайна.	2	
	Практические занятия		**8**	
	1.	Доступ к информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства.	2	
	2	Доступ к информации, составляющей персональные данные	4	
	3.	Доступ к информации при ее предоставлении уполномоченным органам государственной власти.	2	
Тема 5. Составление номенклатуры дел, формирование и оформление конфиденциальных дел.	**Содержание**		**4**	
	1.	Номенклатура конфиденциальных дел	2	
	2	Учет конфиденциальных дел и составление номенклатуры конфиденциальных дел.	2	
	Практические занятия		**6**	
	1.	Учет конфиденциальной информации.	2	
	2.	Формирование конфиденциальных дел.	4	
Тема 6. Подготовка конфиденциальных документов к архивному хранению и уничтожению.	**Содержание**		**8**	
	1.	Экспертиза ценности конфиденциальных документов.	2	
	2.	Подготовка конфиденциальных документов и дел к архивному хранению. Хранение архивных документов	2	
	3.	Подготовка конфиденциальных документов и дел к уничтожению.	2	
	4.	Архивное хранение носителей информации. Уничтожение документов.	2	
	Практические занятия		**8**	
	1.	Экспертиза ценности конфиденциальных документов.	4	
	2.	Подготовка конфиденциальных документов дел ля архивного хранения и уничтожения.	4	

Тема 7. Режим конфиденциальности документированной информации.	**Содержание**		**6**	
	1	Формы обмена конфиденциальной информацией	2	
	2	Режим обмена конфиденциальной документированной информацией.	2	
	3	Учет и регистрация носителей конфиденциальной информации.	2	
	Практические занятия		**8**	
	1.	Обмен конфиденциальной документированной информацией.	4	
	2.	Проверка наличия носителей конфиденциальной информации.	4	
Экзамен по профессиональному модулю				
Самостоятельная работа при изучении раздела 3.			**50**	
Систематическая проработка конспектов занятий, учебной и специальной литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите.				
Тематика внеаудиторной самостоятельной работы Изучение нормативных документов. Выполнение рефераты по темам. Оформление пакета документов, связанных с электронным документооборотом.				
Учебная практика Общие положения концепции обеспечения безопасности информации в системе организации. Угрозы безопасности информации организации. Задачи обеспечения безопасности информации. Принципы построения системы комплексной защиты информации. Участие в планировании и организации работ по обеспечению защиты объекта: Организация и технология работы с конфиденциальными документами Промежуточная аттестация в форме дифференцированного зачета			**72**	
Производственная практика Вводный инструктаж. Организация системы безопасности организации. Изучение механизмов обеспечения безопасности информации. Организация подразделений защиты информации Организация управлением подразделением защиты информации. Определение потенциальных угроз информационной защиты. Работа персонала с конфиденциальной информацией Организация инструктажа персонала			**108**	

Организация контроля персонала. Дифференцированный зачет		
Всего:	**501**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к материально-техническому обеспечению

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

Оборудование учебного кабинета и рабочих мест кабинета:

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

Технические средства обучения:

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

4.2. Информационное обеспечение обучения

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

Основные источники:

1. Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0334-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.
2. Хачатрян, Г. А. Организация и технология работы с конфиденциальными документами : учебник для СПО / Г. А. Хачатрян, И. В. Кузнецова. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2020. — 283 с. — ISBN 978-5-4488-0742-8, 978-5-4497-0783-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.
3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.

Дополнительные источники:

отсутствуют

Интернет-ресурсы:

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

4.3. Кадровое обеспечение образовательного процесса

Реализация ППССЗ обеспечивается педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемой дисциплины (модуля). Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального цикла. Преподаватели получают 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)

Техникум, реализующий подготовку по программе профессионального модуля, обеспечивает организацию и проведение текущего контроля и промежуточной аттестации.

Текущий контроль производится преподавателем в процессе обучения.

По МДК 01.01 Обеспечение организации системы безопасности предприятия, обучающиеся сдают – дифференцированный зачёт.

По МДК 01.02 Организация работ подразделений защиты информации, обучающиеся сдают дифференцированный зачёт.

По МДК 01.03 Организация работы персонала с конфиденциальной информацией, обучающиеся сдают экзамен.

Результатом учебной и производственной практики является дифференцированный зачет.

Обучение по производственному модулю завершается экзаменом по профессиональному модулю, который проводит экзаменационная комиссия.

Формы и методы текущего и итогового контроля по профессиональному модулю самостоятельно разрабатываются техникумом и доводятся до сведения обучающихся не позднее начала двух месяцев от начала обучения.

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.	- определение методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации; - выполнение анализа научной литературы; - обоснование выбора соответствующих решений по защите информации объекта; - обоснование использованных методов обнаружения технических каналов утечки информации	Текущий контроль: - ситуационные задачи, - практические работы, - самостоятельная работа, - защита работ на различных этапах производственной практики, - тестирование.
ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте	- определение предложений по разработке программ защиты информации на объекте; - определение методик защиты информации на предприятии	

ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации	- выполнение работ по защите конфиденциальной информацией; - определение качества защиты информации; - выполнение мероприятий по комплексной защите информации	
ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональнойдеятельности	- обоснование выбранных организационных решений на объектах информатизации; - обоснование мер по внедрению организационных решений на предприятии;	
ПК 1.5. Вести учет, обработку,	-обоснование	
хранение, передачу, использование различных носителей конфиденциальной информации	использования носителей конфиденциальной информации; - определение методики обработки и хранения защищаемой информации; -организация выполнения передачи конфиденциальной информации на различных носителях. - полнота и эффективность соблюдения правил использования носителей секретной информации	
ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий	-определение правил техники безопасности при комплексной защите информации; - определение методики защиты информации при проведении организационно-технических мероприятий.	
ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите	- обоснование выбранных методов проверок организаций, информация которых подлежит защите; - проведение проверки объектов информатизации; - проведение проверки организаций, работающих с конфиденциальной информацией.	

ПК 1.8. Проводить контроль за соблюдением персоналом требований режима защиты информации	- определение методов и способов контроля персонала, работающего с конфиденциальной информацией; - определение последовательности действий при проведении проверок соблюдения персоналом требований режима защиты информации; - организация проведения контроля за работой персонала, задействованного в защите информации организации.	
ПК 1.9. Участвовать в оценке качества защиты объекта	- выполнение оценки качества комплексной защиты информации организации; - выполнение оценки качества защиты объекта информатизации; - определение и анализ недостатков качества защиты информации на предприятии	

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

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.	- демонстрация понимания целей и задач профессиональной деятельности; - осознание способов деятельности, выбор средств, адекватных ее целям и задачам	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методов и способов решения профессиональных задач в организации и технологии защиты информации; - оценка эффективности и качества выполнения работ.	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- рациональность решения стандартных профессиональных задач в области защиты информации; - аргументированность самоанализа выполнения профессиональных задач	
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и	- эффективный поиск необходимой информации; - использование различных источников, включая электронные;	
личностного развития.		
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	- использование программ автоматизации профессиональной деятельности (владеть навыками работы в специальных программах, а также текстовых и табличных редакторах, программах по созданию презентаций).	
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	- взаимодействие с обучающимися, преподавателями, мастерами, руководителями практик от предприятия в ходе обучения	
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	- самоанализ и коррекция результатов собственной работы при выполнении практических заданий в группе, при подготовке к внеклассным мероприятиям	

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	- организация самостоятельных занятий при изучении профессионального модуля	
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	