Автономная некоммерческая профессиональная образовательная организация «Многопрофильная Академия непрерывного образования»
АНПОО «МАНО»
Колледж

ПРИНЯТО
Решением Педагогического совета
АНПОО «МАНО»
Протокол № 01-01/16 от 01.06.2022 г.

УТВЕРЖДАЮ
Ректор АНПОО «МАНО»
_____ В.И. Гам
01 июня 20 22 г.

РАБОЧАЯ ПРОГРАММА
по профессиональному модулю
ПМ.01. Участие в планировании и организации работ по обеспечению защиты объекта
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
УП. 01.01 Учебная практика
ПП.01.01. Производственная практика
Специальность 10.02.01 Организация и технология защиты информации
Квалификация: Техник по защите информации
Заочная форма обучения

Омск, 2022

Рабочая программа профессионального модуля «Участие в планировании и организации работ по обеспечению защиты объекта» разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 10.02.01 Организация и технология защиты информации, утвержденного приказом Министерства образования и науки Российской Федерации от 28 июля 2014 г. № 805.

Организация-разработчик:

АНПОО «Многопрофильная Академия непрерывного образования».

Разработчик:

Гам А.В., преподаватель Колледжа АНПОО «МАНО».

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации в части освоения вида профессиональной деятельности (ВПД): участие в планировании и организации работ по обеспечению защиты объекта.

Программа по профессиональному модулю ПМ. 1. «Участие в планировании и организации работ по обеспечению защиты объекта» содержит МДК. 1.1 «Обеспечение организации системы безопасности предприятия», МДК. 1.2 «Организация работ подразделений защиты информации», МДК. 1.3 «Организация работы персонала с конфиденциальной информацией», УП. 1.01 Учебная практика, ПП.1.01. Производственная практика.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Профессиональный модуль «Участие в планировании и организации работ по обеспечению защиты объекта» входит в профессиональный цикл специальности 10.02.01 «Организация и технология защиты информации».

1.3. Цели и задачи модуля – требования к результатам освоения модуля

В результате изучения профессионального модуля обучающийся 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.

1.4. Количество часов на освоение программы профессионального модуля:

всего - 852 часов, в том числе:

максимальной учебной нагрузки обучающегося – 492 часа, включая

обязательной аудиторной учебной нагрузки обучающегося – 52 часа;

самостоятельной работы обучающегося – 440 часов;

учебной практики - 216 часа;

производственной практики 144 часа.

6. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности «Участие в планировании и организации работ по обеспечению защиты объекта», в том числе общими и профессиональными компетенциями.

5.1 Техник по защите информации должен обладать общими компетенциями, включающими в себя способность:

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.

5.2. Техник по защите информации должен обладать профессиональными компетенциями, соответствующими видам деятельности:

5.2.1. Участие в планировании и организации работ по обеспечению защиты объекта.

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.

6. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

3.1. Тематический план профессионального модуля

Коды профессиональных компетенций	**Наименования разделов профессионального модуля**	**Всего часов** (макс. Учебная нагрузка и практики)	**Обязательная аудиторная учебная нагрузка обучающегося**				**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов если предусмотрена рассредоточенная практика)
			Всего, часов	**в т.ч. лекции**	**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**	**11**
ПК 1.1. – ПК 1.9	**МДК. 1.1 Обеспечение организации системы безопасности предприятия**	**206**	**30**	**12**	**14**	**4**	**176**			
ПК 1.1. – ПК 1.9	**МДК. 1.2 Организация работ подразделений защиты информации**	**142**	**12**	**6**	**6**		**130**			
ПК 1.1. – ПК 1.9	**МДК. 1.3 Организация работы персонала с конфиденциальной информацией**	**144**	**10**	**4**	**6**		**134**			
	Учебная практика	**216**							**216**	
	Производственная практика, часов	**144**								**144**
	Всего:	**852**	**52**	**22**	**26**	**4**	**440**		**216**	**144**

3.2. Содержание обучения по профессиональному модулю ПМ. 1. Участие в планировании и организации работ по обеспечению защиты объекта

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
МДК 1.1 Обеспечение организации систем безопасности предприятия		**30/176**	
Основные понятия безопасности предприятия	**Лекция** **Содержание учебного материала**	2	2
	1. Понятие и содержание безопасности предприятия. Цель обеспечение безопасности предприятия. Виды и способы охраны объекта (предприятия). Особенности охраны персонала организации. Основные направления и методы организации режима и охраны объекта.		
	2. Предмет, объекты и субъекты безопасности предприятия.		
	Самостоятельная работа обучающихся:	6	1,2
	1. Концепция безопасности предприятия.		
	2. Структура концепции безопасности предприятия. Основные положения.		
Виды угроз безопасности предприятия	**Самостоятельная работа обучающихся:**	6	2
	1. Понятие угроз безопасности предприятия и их классификация.		
	2. Сущность и содержание внутренних и внешних угроз безопасности предприятия		
	Самостоятельная работа обучающихся:	4	1,2
	1. Функциональные составляющие обеспечения безопасности предприятия		
Функциональные составляющие обеспечения безопасности предприятия	**Самостоятельная работа обучающихся:**	6	1,2
	1. Основные составляющие системы обеспечения безопасности предприятия		
	2. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.		
	Самостоятельная работа обучающихся:	6	1,2
	1. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание. Информационная безопасность в системе национальной безопасности РФ.		

Информационная безопасность автоматизированных систем	**Самостоятельная работа обучающихся:** 1. Современная постановка задачи защиты информации. Организационно-правовое обеспечение информационной безопасности.	6	2
	Самостоятельная работа обучающихся: 1. Информация как объект юридической защиты. Основные принципы засекречивания информации.	4	1,2
Информационные системы	**Самостоятельная работа обучающихся:** 1. Источники конфиденциальной информации в информационных системах. 2. Виды технических средств информационных систем.	3	1,2
	Самостоятельная работа обучающихся: 1. Общие положения. Информация как продукт. Информационные услуги. 2. Неправомерное овладение конфиденциальной информацией в информационных системах.	3	1,2
Угрозы информации	**Лекция.** **Содержание учебного материала:** 1. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.	4	2
	Практическое занятие. Содержание учебного материала: **Практические задачи:** Учет различных носителей конфиденциальной информации; Обработка различных носителей конфиденциальной информации; Хранение различных носителей конфиденциальной информации; Передача различных носителей конфиденциальной информации; Использование различных носителей конфиденциальной информации. Деловая игра: «Обеспечение техники безопасности при проведении организационно-технических мероприятий».	1	2,3
	Практическое занятие. Содержание учебного материала: Реферат по теме: «Участие в организации и проведении проверок объектов информатизации, подлежащих защите». Решение деловых ситуаций по теме: «Контроль соблюдения персоналом требований режима защиты информации». Составить конспект по теме: «Оценка качества защиты объекта».	1	2,3

	Самостоятельная работа обучающихся:		4	2
	1.	Модель нарушителя информационных систем.		
	Практическое занятие:		2	2,3
	1.	Виды угроз информационным системам.		
	Самостоятельная работа обучающихся		4	1,2
	1.	Убытки, связанные с информационным обменом.		
Методы и модели оценки уязвимости информации	**Самостоятельная работа обучающихся:**		2	2
	1.	Эмпирический подход к оценке уязвимости информации.		
	Самостоятельная работа обучающихся:		4	2
	1.	Практическая реализация модели «угроза – защита».		
Оценки уязвимости информации	**Самостоятельная работа обучающихся:**		6	2,3
	1.	Рекомендации по использованию моделей оценки уязвимости информации, позволяющих определить текущие и прогнозировать будущие значения всех показателей уязвимости информации для любых компонентов автоматизированной системы обработки данных, любой их комбинации и для любых условий жизнедеятельности автоматизированной системы обработки данных.		
Методы определения требований к защите информации	**Самостоятельная работа обучающихся:**		4	2,3
	1.	Требования к защите информации, обусловленные спецификой автоматизированной обработки информации		
	Самостоятельная работа обучающихся:		4	1,2
	1.	Требования, определяемые структурой автоматизированной системы		
Методики определения требований к защите информации	**Самостоятельная работа обучающихся:**		4	2
	1.	Требования к безопасности информационных систем в России.		
	Самостоятельная работа обучающихся:		4	1,2
	1.	Требования к безопасности информационных систем в США.		
	2.	Классы защищенности средств вычислительной техники от несанкционированного доступа.		
	3.	Факторы, влияющие на требуемый уровень защиты информации.		
		Дифференцированный зачет	2	
Функции и задачи зашиты информации	**Лекция.** **Содержание учебного материала**		2	1,2

	1.	Общие положения. Методы формирования функций защиты.		
	2.	Функции защиты. Состояния и функции системы защиты информации.		
	Самостоятельная работа обучающихся:		2	2,3
	1.	Классы задач защиты информации.		
	Лекция. Содержание учебного материала Разрешительная система доступа к конфиденциальной информации Принципы действия аппаратуры систем контроля доступа. Принципы построения и функционирования биометрических систем безопасности. Задачи, функции и структура подразделений защиты информации. Принципы, методы и технология управления подразделений защиты информации. Методы проверки персонала по защите информации. Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.		4	1,2
Стратегии защиты информации	**Самостоятельная работа обучающихся:**		6	2,3
	1.	Организация защиты информации. Подготовка докладов и презентаций: 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. Организация работы при осуществлении международного сотрудничества. Требования режима защиты информации в процессе рекламной деятельности. Требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.		
	2.	Уровень технологических схем обработки.		
	Практические занятия:		4	1,2,3
	1.	Уровень структурно-организационного построения объекта обработки информации.		
	2.	Виды стратегии защиты информации. Практические задания по использованию физических средств защиты объекта. Применение физических средств контроля доступа на объект. Текущая работа исполнителей с конфиденциальной информацией.		
Архитектура систем защиты информации	**Самостоятельная работа обучающихся:**		10	2
	1.	Ресурсы системы защиты информации. Организационное построение.		
	2.	Криптографические методы и средства защиты информации в компьютерных системах и сетях		

	3.	Комплексная защита информации в компьютерных системах и сетях.		
	4.	Безопасность сетевых операционных систем		
	5.	Безопасность локальных и глобальных сетевых технологий		
	Практическое занятие. **Содержание учебного материала:** Разработать программу и методику организации защиты информации на объекте (объект выбирает обучающийся). Индивидуальный проект по планированию и организации выполнения мероприятий по защите информации.		2	2,3
Экономическая безопасность предприятия	**Самостоятельная работа обучающихся:**		12	2,3
	1.	Типичная структура экономической безопасности предприятия		
	2.	Трансформация структуры обеспечения экономической безопасности предприятия		
	3.	Уровни экономической безопасности		
	4.	Национальная экономическая безопасность		
	5.	Угрозы экономической безопасности		
	6.	Показатели и индикаторы экономической безопасности предприятия		
	7.	Классификация и оценка экономической безопасности		
	8.	Характеристика состояния экономической безопасности современного предприятия		
	9.	Мониторинг экономической безопасности предприятия. Основные цели мониторинга экономической безопасности предприятия		
	Практическое занятие. **Содержание учебного материала:** Сбор и обработка материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. Разработать план внедрения разработанных организационных решений на объектах профессиональной деятельности.		2	2,3
Обеспечение экономической безопасности	**Самостоятельная работа обучающихся:**		10	2,3
	1.	Функциональные составляющие экономической безопасности		
	2.	Корпоративные ресурсы экономической безопасности предприятия		
	3.	Основные подходы к формированию экономической безопасности предприятия		
	4.	Сущность финансовой составляющей экономической безопасности предприятия.		

	5.	Основные индикаторы состояния финансовой составляющей экономической безопасности предприятия.		
	6.	Способы обеспечения финансовой составляющей экономической безопасности предприятия.		
Отечественные и международные акты обеспечения ИБ	**Самостоятельная работа обучающихся:**		4	2
	1.	Отечественное организационное и нормативно-правовое обеспечение ИБ		
	2.	Международное нормативно-правовое обеспечение ИБ		
	3.	Проведение аудита состояния информационной безопасности		
	4.	Определение уязвимостей информационной системы		
	5.	Расчет коэффициентов авторитета экспертов		
Организационное регулирование защиты процессов переработки информации	**Самостоятельная работа обучающихся:**		4	2
	1.	Категорирование объектов и защиты информационных систем		
	2.	Ответственность за нарушение законодательства в информационной сфере		
	3.	Анализ и оценка концепций защиты процессов переработки информации		
	Самостоятельная работа обучающихся:		4	2,3
	1.	Построение матрицы парных сравнений уязвимостей		
	2.	Составление вектора доступности уязвимостей		
Организация противодействия технической разведке	**Самостоятельная работа обучающихся:**		4	2
	Организация противодействия технической разведке. Защита от утечки информации, несанкционированного доступа. Составление матрицы причинно-следственных связей			
Методологические основы технического обеспечения защиты процессов переработки информации и контроля ее эффективности	**Самостоятельная работа обучающихся:**		8	2
	1.	Методологические основы технического обеспечения защиты процессов переработки информации и контроля ее эффективности		
	2.	Системная организация оповещения о попытках вторжения		
	3.	Системы опознавания нарушителей		
	4.	Механическая защита объекта		
	5.	Автоматизация технического контроля защиты потоков информации.		
	Самостоятельная работа обучающихся:		4	2,3
	1.	Расчет вероятностей возникновения угроз безопасности		
	2.	Расчет степени воздействия угроз		

	3.	Составление перечня защищаемых информационных ресурсов		
Программно-аппаратные средства защиты ПЭВМ	**Самостоятельная работа обучающихся:**		4	2
	1.	Методы и средства ограничения и доступа к компонентам ЭВМ		
	2.	Программно-аппаратные средства защиты ЭВМ		
	Самостоятельная работа обучающихся:		4	1,2,3
	1.	Составление списка элементов информационной системы предприятия		
	2.	Составление списка элементов системы защиты информации		
Методы и средства обеспечения хранения и переработки ключевой и другой информации	**Самостоятельная работа обучающихся:**		4	2,3
	Методы и средства обеспечения хранения и переработки ключевой и другой информации Составление перечня количественных и качественных требований к системе защиты информации Расчет основных показателей экономической эффективности системы защиты информации			
Защита программного обеспечения от изучения, вирусного заражения, разрушающих программных действий	**Самостоятельная работа обучающихся:**		10	1,2,3
	1.	Основные классификационные признаки компьютерных вирусов		
	2.	Некоторые компьютерные вирусы		
	3.	Методы и технологии борьбы с компьютерными вирусами		
	4.	Условия безопасной работы компьютерных систем и технология обнаружения заражения вирусами		
	5.	Контроль целостности и системные вопросы защиты программ и данных		
	6.	Оценка ценности информационных активов предприятия		
	7.	Разработка концепции информационной безопасности предприятия		
Программно-аппаратные средства обеспечения ИБ в типовых ОС, СУБД, вычислительных сетях	**Самостоятельная работа обучающихся:**		6	1,2,3
	1.	Основные положения программно-аппаратного и организационного обеспечения ИБ в операционных системах		
	2.	Защита процессов переработки информации в СУБД		
	3.	Программно-аппаратные средства обеспечения ИБ в вычислительных сетях. Работа с приложениями GlassWire, Click&Clean, StartPage, uBlock.		

	4.	Механизмы проверки целостности данных		
	5.	Схема шифрования Эль-Гамаля		
	6.	Механизмы проверки подлинности ЭЦП		
Тематика курсового проектирования: 1. Оценка угроз безопасности информации в информационной системе организации при несанкционированном доступе (на примере организации). 2. Анализ угроз и уязвимостей информации в организации от ее утечки по техническим каналам. 3. Организация инженерно-технической охраны объектов. 4. Организация защиты информации в локальной сети организации от несанкционированного доступа. 5. Программно-аппаратные средства защиты информации в локальной вычислительной сети организации от несанкционированного доступа. 6. Программно-аппаратные средства защиты информации в интранет-сети организации от несанкционированного доступа. 7. Организация и администрирование пропускного режима в организации (на примере организации). 8. Построение комплексной системы защиты информации в организации (на примере организации). 9. Анализ и оценка рисков безопасности информации в организации от утечки по техническим каналам. 10. Анализ и оценка рисков безопасности информации в ЛВС организации от несанкционированного доступа. 11. Анализ и оценка рисков безопасности информации в интранет-сети организации от несанкционированного доступа. 12. Установление режима коммерческой тайны в организации. 13. Разработка политики информационной безопасности в организации (на примере организации). 14. Разработка программы проведения аудита безопасности информации в организации (на примере организации). 15. Организация и проведение конфиденциальных переговоров в организации. 16. Разработка мероприятий по контролю эффективности функционирования системы защиты информации в компании. 17. Разработка комплекса мер по защите информации от утечки по техническим каналам в организации. 18. Контроль мероприятий по защите информации от НСД на предприятиях различных форм собственности. 19. Разработка предложений по созданию комплексной системы защиты информации в организации.			**4**	

20. Формирование системы управления информационной безопасностью в организации (компании). 21. Организация обработки персональных данных в компании (организации). 22. Состав и содержание мер по обеспечению безопасности персональных данных в организации. 23. Порядок определения сведений, составляющих коммерческую тайну. 24. Порядок организации защиты информации, составляющей коммерческую тайну. 25. Методы и способы защиты информации от утечки по техническим каналам в переговорной комнате организации. 26. Методы и средства защиты информации от несанкционированного доступа в сети Интернет. 27. Разработка предложений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. 28. Разработка предложений по обеспечению безопасности информации в автоматизированных системах управления технологическими процессами. 29. Комплексная система обеспечения информационной безопасности как сложная организационно-иерархическая система. 30. Функции руководства и подразделений хозяйствующего субъекта и службы защиты информации по обеспечению информационной безопасности. 31. Методика выявления состава носителей защищаемой информации. 32. Состав средств обеспечения функционирования хозяйствующего субъекта, подлежащих защите. Факторы, определяющие необходимость защиты периметра и здания предприятия. 33. Анализ требований международных и российских стандартов в области информационной безопасности. 34. Политика ИБ как методологическая основа функционирования хозяйствующего субъекта. 35. Направления деятельности кадрового обеспечения. Основные мероприятия в области обеспечения информационной безопасности, проводимые при подборе, в процессе работы и при увольнении сотрудников. 36. Оценка степени уязвимости информации в результате действий нарушителей различных категорий 37. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость их от структуры предприятия, защищаемых элементов объектов, условий функционирования комплексной системы обеспечения информационной безопасности хозяйствующего субъекта. 38. Порядок выбора структуры комплексной системы обеспечения информационной безопасности хозяйствующего субъекта, ее зависимость от объектов защиты, характера и условий функционирования хозяйствующего субъекта 39. Сущность процессов управления комплексной системой обеспечения информационной		

безопасности хозяйствующего субъекта. 40. Организация проведения аудита информационной безопасности хозяйствующего субъекта. Программные средства для анализа рисков информационной безопасности. 41. Оценочный подход на основе формирования требований к защищенности объекта: классы защищенности и их характеристика, контрольно-испытательные процедуры определения соответствия защиты установленным требованиям 42. Области применения и анализ приемлемости различных методов и моделей для решения задачи оценки эффективности комплексной системы информационной безопасности хозяйствующего субъекта.				
Экзамен				
МДК 1.2 Организация работ подразделений защиты информации			**12/130**	
Место и роль службы защиты информации в системе защиты информации	**Лекция.** **Содержание учебного материала:**		**2**	2
	1.	Назначение службы защиты информации. Задачи, функции и структура подразделений защиты информации. Принципы, методы и технология управления подразделений защиты информации. Методы проверки персонала по защите информации. Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.		
	Самостоятельная работа обучающихся		16	
	1.	Место службы защиты информации в системе безопасности предприятия		
	2.	Служба защиты информации как составляющая часть системы зашиты информации		
	3.	Служба защиты информации как орган управления защитой информации		
	4.	Статус службы защиты информации в структуре безопасности предприятия		
	5.	Разработка организационно-правовых аспектов деятельности службы защиты информации		
Основные задачи и функции службы защиты информации	**Самостоятельная работа обучающихся**		**8**	2
	1.	Организационные задачи и функции службы зашиты информации		
	2.	Технологические задачи и функции службы защиты информации		
	3.	Координационные задачи и функции службы защиты информации		
	4.	Разработка организационной структуры службы защиты информации		
Общая структура и штаты службы защиты	**Самостоятельная работа обучающихся**		**10**	2,3
	1.	Общая структурная схема службы защиты информации		

информации	2.	Подразделения службы защиты информации		
	3.	Факторы, определяющие конкретную структуру службы защиты информации		
	4.	Виды и типы организационных структур службы защиты информации		
	5.	Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ		
	6.	Задачи, функции, права и ответственность заместителя руководителя предприятия по безопасности в области защиты информации		
	7.	Разработка модели системы защиты информации для службы защиты информации		
	8.	Место и роль службы защиты информации в системе защиты информации		
	9.	Задачи и функции службы защиты информации		
	10.	Структура и штаты службы защиты информации		
	1.	Организация охраны персонала, территорий, зданий, помещений и продукции организации. Составить сравнительную таблицу: «Аппаратура систем контроля доступа». Практические задачи на выделение зоны доступа по типу и степени конфиденциальности работ.	10	2,3
	2.	Подготовка рефератов по следующим темам: 1. Требования и особенности оборудования режимных помещений; 2. Требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров; 3. Требования режима защиты информации при приеме в организации посетителей; 4. Организация работы при осуществлении международного сотрудничества; 5. Требования режима защиты информации в процессе рекламной деятельности; 6. Требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;		
Организационные основы и принципы деятельности службы защиты информации	**Самостоятельная работа обучающихся**		**18**	2
	1.	Порядок создания службы защиты информации		
	2.	Структура и содержание положения о службе защиты информации		
	3.	Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации		
	4.	Основные принципы организации и деятельности службы защиты информации		
	5.	Экспертная оценка мероприятий по защите информации в службе защиты информации		

	6.	Организация работы с персоналом, имеющим доступ к конфиденциальной информации. Проведение инструктажа персонала по организации работы с конфиденциальной информацией. Контроль соблюдения персоналом требований режима защиты информации (решение практических задач).		
	7.	Подбор, расстановка кадров и обучение сотрудников службы защиты информации Составить краткий конспект по теме: «Критерии подбора и расстановки сотрудников подразделений защиты информации». Анализ деловых ситуаций.		
	8.	Организационные основы и принципы деятельности службы защиты информации		
	9.	Оценка производительности труда по результатам оптимизации процессов в службе защиты информации		
Подбор, расстановка и обучение сотрудников службы защиты информации	**Лекция.** **Содержание учебного материала:**		4	2
	1.	Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации		
	Самостоятельная работа обучающихся		12	1,2,3
	1.	Особенности подбора кадров		
	2.	Методы получения информации о кандидатурах на должности.		
	3.	Формы повышения квалификации сотрудников. Подготовка кадрового резерва		
	4.	Мониторинг и корректировка внутренних мер по защите информации в службе защиты информации		
	5.	Анализ деловых ситуаций по теме: «Внедрение организационных решений на объектах профессиональной деятельности».		
	1.	Принципы и методы управления службой защиты информации	12	1,2,3
	2.	Технология управления службой защиты информации		
	3.	Состав и характеристика процесса проектирования деятельности службы защиты информации		
	4.	Методы организационного проектирования деятельности службы защиты информации. Индивидуальный проект: «Планирование и организация выполнения мероприятий по защите информации».		
Организация труда сотрудников службы защиты информации	**Практическое занятие:**		2	2
	1.	Специфика деятельности сотрудников службы защиты информации. Изучить специфику ведения текущей работы исполнителей с конфиденциальной информацией.		

		Анализ деловых ситуаций: «Порядок организации и проведения рабочих совещаний». Методы защиты информации в рекламной и выставочной деятельности. Практическая работа по использованию физических средств защиты объекта. Составить таблицу «Физические средства контроля доступа на объект».		
	Самостоятельная работа обучающихся		12	
	1.	Распределение обязанностей между сотрудниками службы защиты информации		
	2.	Структура и содержание должностных инструкций сотрудников службы защиты информации.		
	3.	Организация рабочих мест сотрудников службы зашиты информации		
	Практическое занятие **Содержание учебного материала:** Сбор и обработка материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. Выполнение индивидуального проекта: разработать программу и методику организации защиты информации на объекте.		2	3
Принципы и методы управления службой защиты информации	**Самостоятельная работа обучающихся**		**16**	2
	1.	Принципы управления службой защиты информации		
	2.	Система методов управления.		
	3.	Взаимосвязь методов управления		
	4.	Необходимость комплексного и системного применения методов управления службой защиты информации.		
	5.	Понятие и сущность методов управления.		
	6.	Административно-правовые методы управления.		
	7.	Экономические методы управления.		
	8.	Социально-психологические методы управления.		
Технология управления службой защиты информации	**Самостоятельная работа обучающихся**		**16**	2
	1.	Экономические методы управления. Социально-психологические методы управления.		
	2.	Технология управления службой защиты информации.		
	3.	Значение управленческих решений		
	4.	Цели планирования		
	5.	Критерии эффективности службы защиты информации.		

	6.	Пути и способы повышения эффективности управления службой защиты информации.		
	7	Мероприятия по мониторингу направлений деятельности службы защиты информации		
		Дифференцированный зачет	2	
МДК 1.3. Организация работы персонала с конфиденциальной информацией			**10/134**	
Понятие о конфиденциальных документах	**Лекция** **Содержание учебного материала:**		**2**	1,2
	1.	Общие положения. Классификация информации и документов по категориям доступа. Организация охраны персонала, территорий, зданий, помещений и продукции организаций. Использование аппаратуры систем контроля доступа. Выделение зоны доступа по типу и степени конфиденциальности работ.		
	Самостоятельная работа обучающихся:		**16**	1,2,3
	1.	Понятие ценной и конфиденциальной информации. Перечень сведений конфиденциального характера		
	2.	Представление и распространение информации. Персональные данные		
	3.	Тайна следствия и судопроизводства. Служебная тайна. Профессиональная тайна. Коммерческая тайна. Ноу-хау.		
	4.	Нормативная база конфиденциального делопроизводства.		
	5.	Обработка персональных данных без использования средств информатизации.		
	6.	Нормативно-правовая база организации работы с конфиденциальными документами.		
Особенности работы с конфиденциальной информацией	**Самостоятельная работа обучающихся:**		**20**	1,2,3
	1.	Особенности документирование конфиденциальной информации.		
	2.	Оформление реквизитов конфиденциальных документов при документировании информации.		
	3.	Ограничение доступа к документам и использование отметки конфиденциальности при оформлении документов.		
	4.	Перечень конфиденциальной информации.		
	5.	Основные этапы разработки перечня конфиденциальной документированной информации.		

	6.	Учет бумажных носителей информации и их проектов.		
	7.	Разработка перечня документированной конфиденциальной информации.		
	8.	Определение степени разграничения доступа к документам и использование отметки конфиденциальности при оформлении документов.		
Особенности организации конфиденциального документооборота	**Самостоятельная работа обучающихся:**		**20**	1, 2, 3
	1.	Учет и регистрация конфиденциальной документированной информации.		
	2.	Обработка поступающих конфиденциальных документов, их учет и регистрация.		
	3.	Технология исполнения и контроля за исполнением конфиденциальных документов.		
	4.	Учет и регистрация внутренних, исходящих и внешних конфиденциальных документов.		
	5.	Учет конфиденциальной документированной информации выделенного хранения.		
	6.	Обработка поступающих и внутренних конфиденциальных документов, их учет и регистрация.		
	7.	Учет и регистрация внутренних конфиденциальных документов.		
	8.	Исполнение и контроль за исполнением конфиденциальных документов.		
Текущая работа с персоналом, обладающим конфиденциальной информацией	**Самостоятельная работа обучающихся:**		**10**	1,2,3
	1.	Профессиональная ориентация и обучение персонала		
	2.	Мотивация персонала к выполнению требований по защите информации.		
	3.	Методы работы с персоналом и их характеристика. Методы проверки персонала по защите информации. Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.		
Текущая работа с персоналом, обладающим конфиденциальной информацией	**Лекция.** **Содержание учебного материала:**		**2**	
	1.	Подбор персонала на должности, связанные с работой с конфиденциальной информацией. Критерии подбора и расстановки сотрудников подразделений защиты информации. Специфика текущей работы исполнителей с конфиденциальной информацией.		
	Самостоятельная работа обучающихся:		**18**	
	1.	Допуск к секретной информации.		
	2.	Нормативно-методическая база организации работы с документами, содержащими служебную тайну.		
	3.	Порядок определения перечня предметов, запрещенных к проносу провозу на		

		режимную территорию. Общие требования внутри объектового режима.		
	4.	Экспедиционные технологии обработки и учета поступающих пакетов с конфиденциальной информацией		
	5.	Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта.		
	6.	Порядок допуска работников в помещения, где ведутся конфиденциальные работы.		
	Практическое занятие:		**2**	2,3
	1.	Деловая игра: «Организация работы с персоналом, имеющим доступ к конфиденциальной информации». Проведение инструктажа персонала по организации работы с конфиденциальной информацией. Контроль соблюдения персоналом требований режима защиты информации. Ведение учета, обработки, хранения, передачи, использования различных носителей конфиденциальной информации (решение практических задач).		
Охрана территории, зданий, помещений и персонала	**Самостоятельная работа обучающихся:**		**15**	1,2,3
	1.	Понятие «охрана». Цели и задачи охраны. Виды и способы охраны объекта. Особенности охраны персонала организации. Основные направления и методы организации режима и охраны объекта. Разрешительная система доступа к конфиденциальной информации. Принципы действия аппаратуры систем контроля доступа. Принципы построения и функционирования биометрических систем безопасности. Требования и особенности оборудования режимных помещений.		
	2.	Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия		
	3.	Порядок назначения комиссии для аттестации помещений на пригодность их для ведения конфиденциальных работ		
	4.	Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных изделий и документов		
Организация пропускного и внутри объектового режимов	**Самостоятельная работа обучающихся:**		**17**	1,2,3
	1.	Понятие «пропускной режим». Цели и задачи пропускного режима. Особенности охраны персонала.		
	2.	Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков.		
	3.	Организация подготовки и проведения совещаний и переговоров. Требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по		

		конфиденциальным вопросам и переговоров;		
	4.	Организация защиты информации при приеме в организации посетителей и командированных лиц. Требования режима защиты информации при приеме в организации посетителей.		
	5.	Организация защиты информации при приеме в организации иностранных представителей. Организация работы при осуществлении международного сотрудничества;		
	Практическое занятие. **Содержание учебного материала:** Сбор и обработка материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. Составить таблицу «Каналы утечки информации». Разработать ряд мероприятий по защите информации (индивидуальное задание).		2	2,3
Подготовка и проведение совещаний и переговоров по конфиденциальным вопросам	**Самостоятельная работа обучающихся:**		**18**	1,2,3
	1.	Основные требования, предъявляемые к подготовке и проведению совещаний и переговоров по конфиденциальным вопросам. Порядок назначения ответственных лиц и их обязанности по проведению совещаний и переговоров.		
	2.	Организация защиты информации при осуществлении рекламной выставочной и публикаторской деятельности. Требования режима защиты информации в процессе рекламной деятельности.		
	3.	Организация защиты информации при подготовке материалов к открытому опубликованию. Требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.		
	4.	Аналитическая работа как основа управления системой организационной защиты информации.		
	5.	Планирование процессов организационной защиты информации.		
	6.	Контроль функционирования системы организационной защиты информации.		
			Дифференцированный зачет	**2**
Учебная практика **Задание:**			**216**	

Ознакомление с предприятием и рабочими местами. 1. Задачи и краткое содержание учебной практики по специальности. 2. Инструктаж по общим вопросам, охране труда и технике безопасности, по режиму работы предприятия. 3. Изучение структуры предприятия и взаимосвязи подразделений. Основная деятельность предприятия. **Обеспечение организации системы безопасности предприятия** 1. Организационно-штатная структура службы корпоративной безопасности. 2. Основные функциональные цели и задачи службы корпоративной безопасности. 3. Функциональные подразделения: их штатная структура. **Организация работ подразделений защиты информации** 1. Виды конфиденциальной информации организации. 2. Кадровая безопасность организации. **Организация работы персонала с конфиденциальной информацией** 1. Активный и пассивный доступ к информационным ресурсам. Проблемы, возникающие при реализации правовых мер защиты информации. 2. Система сбора и накопления информации. 3. Информационные базы. 4. Система переработки информации.		
Производственная практика (по профилю специальности) Задание: **Ознакомление с предприятием и рабочими местами.** 4. Задачи и краткое содержание производственной практики по специальности. 5. Инструктаж по общим вопросам, охране труда и технике безопасности, по режиму работы предприятия. 6. Изучение структуры предприятия и взаимосвязи подразделений. Основная деятельность предприятия. **Обеспечение организации системы безопасности предприятия** 1. Организация управленческой и функциональной деятельности службы корпоративной безопасности. 2. Взаимодействие службы защиты корпоративных интересов с кадровыми службами. 3. Технические средства контроля доступа и безопасности. 4. Основные критерии защищенности информационных автоматизированных систем.	**144**	

Организация работ подразделений защиты информации 1. Организационно-штатная структура службы корпоративной безопасности. 2. Основные функциональные цели и задачи службы корпоративной безопасности. 3. Функциональные подразделения: их штатная структура. **Организация работы персонала** с **конфиденциальной информацией** 1. Анализ угроз информационной безопасности. 2. Защита представления информации. 3. Защита содержания информации. 4. Построение системы защиты от угрозы доступности информации.		
Итоговый контроль по ПМ. 1. Участие в планировании и организации работ по обеспечению защиты объекта: квалификационный экзамен		
Всего часов с учетом практик	**852**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (узнавание ранее изученных объектов, свойств);
2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация профессионального модуля предполагает наличие учебного кабинета по профилю специальности.

Оборудование учебного кабинета:

- мебель по количеству студентов;
- доска;
- наглядные пособия, дидактические средства.

Технические средства обучения:

- персональный компьютер;
- мультимедиа-проектор;
- программное обеспечение (Linux Mint, Apache OpenOffice, Kaspersky Anti-Virus (Пробная версия), Консультант Плюс, браузер).

4.2. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОБУЧЕНИЯ

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование).

2. *Казарин, О. В.* Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование).

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование).

4. *Внуков, А. А.* Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование).

Дополнительные источники:

1. Партыка Т.Л., Попов И.И. Информационная безопасность. М.: Форум,2011

2. Безопасность и упр.доступ. в информ. сист.: Уч.пос. /Васильков А.В., Васильков И.А.-М.:Форум, НИЦ ИНФРА-М, 2017-368с. - 978-5-91134-360-6.

3. Информационная безопасность компьютерных систем и сетей: Уч. пос./В.Ф.Шаньгин -М.: ИД ФОРУМ, НИЦ ИНФРА-М,2018-416с (ПО) ISBN:978-5-8199-0754-2.

4. Аксеров Т.М. Защита информации и информационная безопасность. М.:Рос.экон.акад., 2011.

5. Колмогоров А.Н. Безопасность предприятия. М.: Академия, 2010

6. Васильева И.Н., Стельмашонок Е.В. Информационные технологии и защита информации. Учебное пособие. - СПб, СП6ГИЭУ,2011

7. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. Учебное пособие. - М.: Форум: Инфра-М, 2010.

8. В.И. Аверченков, М.Ю. Рытов. Организационная защита информации: учеб. пособие. М.: Флинта, 2011. - 184 с.

9. О.А. Романов, С.А. Бабин, С.Г. Жданов. Организационное обеспечение информационной безопасности: учебник. М.: Академия, 2010. - 192 с.

10.Завгородний В.И. Комплексная защита информации. М.:Логос, 2011

11.Собрание законодательства РФ от 20 февраля 1995. Федеральный закон «Об информации, информатизации и защите информации». М.: «Юридическая литература», 2012

12.Васильева И.Н. Защита информации. СПб.: СПбГИЭУ, 2010

13.Галатенко В. А. Стандарты информационной безопасности. М.: Интернет-Университет Информационных Технологий - ИНТУИТ.РУ, 2010

14.Гаценко О.Ю. Защита информации. СПб.: Изд. дом "Сентябрь", 2011.

15.В.П. Мельников, С.А. Клейменов. Информационная безопасность и защита информации. М.: Академия, 2010. - 336 с.

16.СП. Расторгуев. Основы информационной безопасности. М.: Академия, 2010. – 192 с.

4.3. ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Освоение программы модуля базируется на изучении общепрофессиональных дисциплин «Документационное обеспечение управления», «Основы информационной безопасности», «Технические средства информатизации».

Реализация программы модуля предполагает учебную и производственную практики, которые проводятся концентрированно в соответствии с освоением всех разделов модуля. Практика проводится с целью закрепления и углубления теоретических знаний, а также формирования у обучающихся профессиональных компетенций.

Обязательным условием допуска к производственной практике в рамках профессионального модуля является освоение междисциплинарного курса «Участие в планировании и организации работ по обеспечению защиты объекта». Аттестация по итогам практики проводится на основании результатов, подтверждаемых отчётами и дневниками практики студентов, а также отзывами руководителей практики на студентов.

Учебная и производственная практики завершаются зачётом освоенных общих и профессиональных компетенций.

Изучение программы модуля завершается итоговой аттестацией, результаты которой оцениваются в форме квалификационного экзамена по модулю.

4.4. КАДРОВОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

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

- наличие высшего профессионального образования, соответствующего профилю модуля;
- опыт деятельности в организациях соответствующей профессиональной сферы;

- преподаватели должны проходить стажировку в профильных организациях не реже 1 раза в 3 года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: дипломированные специалисты – преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин.

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

Образовательная организация, реализующая подготовку по программе данного профессионального модуля, обеспечивает организацию и проведение текущего контроля индивидуальных образовательных достижений – демонстрируемых обучающимися знаний, умений и навыков.

Текущий контроль проводится преподавателем в процессе обучения.

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе проведения устных опросов, тестирования, практических занятий, а также выполнения обучающимися индивидуальных и групповых заданий. Аттестация по модулю в целом проводится в форме квалификационного экзамена.

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

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.	- 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 учебной, производственной практики.
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	Текущий контроль: - тестирование, - практические работы, - самостоятельная работа, - защита работ на различных этапах учебной, производственной

		практики.
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	Текущий контроль: - ситуационные задачи, - тестирование, - практические работы, - самостоятельная работа, - защита работ на различных этапах учебной, производственной практики.
ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности	- обоснование выбранных организационных решений на объектах информатизации; - обоснование мер по внедрению организационных решений на предприятии;	Текущий контроль: - ситуационные задачи, - тестирование, - практические работы, - самостоятельная работа, - защита работ на различных этапах учебной, производственной практики.
ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации	обоснование использования носителей конфиденциальной информации; - определение методики обработки и хранения защищаемой информации; - организация выполнения передачи конфиденциальной информации на различных носителях. - полнота и эффективность соблюдения правил использования носителей секретной информации	Текущий контроль: - ситуационные задачи, - тестирование, - практические работы, - самостоятельная работа, - защит работ на различных этапах учебной, производственной практики.
ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий	определение правил техники безопасности при комплексной защите информации; определение методики защиты информации при проведении организационно- технических мероприятий.	Текущий контроль: - ситуационные задачи, - тестирование, - практические работы, - самостоятельная работа, защит работ на различных этапах учебной, производственной практики.
ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите	- обоснование выбранных методов проверок организаций, информация которых подлежит защите; - проведение проверки объектов информатизации; - проведение проверки организаций, работающих с конфиденциальной информацией.	Текущий контроль: - ситуационные задачи, - тестирование, - практические работы, - самостоятельная работа, защит работ на различных этапах учебной, производственной практики.
ПК 1.8. Проводить контроль за соблюдением персоналом требований режима защиты информации	- определение методов и способов контроля персонала, работающего с конфиденциальной информацией; - определение последовательности действий при проведении проверок соблюдения	Текущий контроль: - ситуационные задачи, - тестирование, - практические работы,

	персоналом требований режима защиты информации; - организация проведения контроля за работой персонала, задействованного в защите информации организации.	- самостоятельная работа, защит работ на различных этапах учебной, производственной практики.
ПК 1.9. Участвовать в оценке качества защиты объекта	- выполнение оценки качества комплексной защиты информации организации; - выполнение оценки качества защиты объекта информатизации; - определение и анализ недостатков качества защиты информации на предприятии.	Текущий контроль: - ситуационные задачи, - тестирование, - практические работы, - самостоятельная работа, защит работ на различных этапах учебной, производственной практики.

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

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
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	- тестирование, - практические работы, - самостоятельная работа, - защита работ на различных этапах производственной практики
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 личностного развития.	- эффективный поиск необходимой информации; - использование различных источников, включая электронные	
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности	- использование программ автоматизации профессиональной деятельности	

	(владеть навыками работы в специальных программах, а также текстовых и табличных редакторах, программах по созданию презентаций).	
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	- взаимодействие с обучающимися, преподавателями, мастерами, руководителями практик от предприятия в ходе обучения	
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий	- самоанализ и коррекция результатов собственной работы при выполнении практических заданий в группе, при подготовке к внеклассным мероприятиям	
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознано 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.	- уметь применять средства математической логики для решения задач	
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности	- уметь оценивать документы, используемые в области защиты информации	
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность	- проявление интереса к структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	

ВОПРОСЫ ИТОГОВОГО КОНТРОЛЯ

МДК. 1.1 Обеспечение организации системы безопасности предприятия

1. Средства и методы обеспечения безопасности предприятия.
2. Критерии безопасности предприятия.
3. Определение и содержание наиболее важных показателей безопасности предприятия.
4. Основные направления и способы обеспечения безопасности предприятия.
5. Построение эффективной системы безопасности предприятия.
6. Диагностическое обследование системы безопасности предприятия.
7. Последовательность работ при проведении аудита системы безопасности предприятия.
8. Виды и способы охраны объекта.
9. Особенности охраны персонала организации.
10. Основные направления и методы организации режима и охраны объекта.
11. Разрешительная система доступа к конфиденциальной информации.
12. Принципы действия аппаратуры систем контроля доступа.
13. Принципы построения и функционирования биометрических систем безопасности.
14. Требования и особенности оборудования режимных помещений.
15. Требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров.
16. Требования режима защиты информации при приеме в организации посетителей.
17. Организация работы при осуществлении международного сотрудничества.
18. Требования режима защиты информации в процессе рекламной деятельности.
19. Требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.

20. Задачи, функции и структуру подразделений защиты информации.

21. Принципы, методы и технологию управления подразделений защиты информации.

22. Методы проверки персонала по защите информации;

23. Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.

24. Государственная информационная политика.

25. Проблемы информационной войны.

26. Проблемы информационной безопасности в сфере государственного и муниципального управления.

27. Государственная система правового обеспечения защиты информации в РФ.

28. Государственная информационная безопасность РФ.

29. Законодательство в области информационной безопасности.

30. Радиоэлектронные системы и устройства защиты информации.

31. Виды потерь.

32. Информационные инфекции.

33. Система с полным перекрытием.

34. Политика и модели безопасности.

35. Требования, связанные с размещением защищаемой информации.

36. Требования, обусловленные видом защищаемой информации.

37. Анализ существующих методик определения требований к защите информации.

38. Оценка состояния безопасности ИС. Критерии оценки безопасности информационных технологий.

39. Методы защиты информации.

40. Средства защиты информации.

41. Требования к криптосистемам. Основные алгоритмы шифрования.

42. Цифровые подписи. Криптографические хеш-функции.

43. Криптографические генераторы случайных чисел.

44. Криптоанализ и атаки на криптосистемы.

45. Требования к архитектуре систем защиты информации. Построение систем защиты информации.

46. Ядро системы защиты информации.

47. Управление безопасностью на основе интеграции. Обеспечение безопасности современного предприятия.

48. Использование единого информационного пространства при организации управления безопасностью.

49. Структура единого информационного пространства.

50. Обобщенная архитектура системы управления безопасностью предприятия.

51. Алгоритмы управления безопасностью.

52. Оценка и управление рисками.

53. Управление безопасностью.

54. Алгоритм управление безопасностью.

55. Автоматизированная система управления безопасностью.

56. Модель базы данных системы информационной безопасности предприятия.

57. Метод CRAMM анализа рисков.

58. Программное обеспечение Risk Watch.

59. Модель вероятного нарушителя информационной безопасности.

60. Описание объектов и целей реализации угроз информационной безопасности.

61. Средства защиты денежных средств, материальных ценностей и документации.

62. Проверка лояльности персонала организации.

63. Система кондиционирования воздуха как составная часть безопасности предприятия.

64. Системы охранной и пожарной сигнализации.

65. Сбор и обработка материалов для выработки решений по обеспечению

защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.

66. Алгоритм разработки программ и методик организации защиты информации на объекте.

67. Планирование и организация выполнения мероприятий по защите информации.

МДК. 1.2 Организация работ подразделений защиты информации

1. Оптимизация структуры управления службой защиты информации.
2. Мероприятия по контролю и мониторингу направлений деятельности службы защиты информации.
3. Мероприятия по мониторингу направлений деятельности службы защиты информации.
4. Взаимосвязь и соотношение организационных, технологических и координационных задач и функций.
5. Факторы, влияющие на определение задач и функций службы защиты информации.
6. Централизованная и децентрализованная структуры службы защиты информации, условия, критерии, определяющие выбор структур.
7. Факторы, определяющие численность сотрудников службы защиты информации.
8. Оценка эффективности работы службы защиты информации.
9. Условия и факторы, влияющие на организацию работы службы защиты информации.
10. Организация взаимодействия службы защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации.
11. Виды и способы охраны объекта.
12. Особенности охраны персонала организации.
13. Основные направления и методы организации режима и охраны объекта.
14. Разрешительная система доступа к конфиденциальной информации.

15. Принципы действия аппаратуры систем контроля доступа.
16. Принципы построения и функционирования биометрических систем безопасности.
17. Требования и особенности оборудования режимных помещений.
18. Требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров.
19. Требования режима защиты информации при приеме в организации посетителей.
20. Организация работы при осуществлении международного сотрудничества.
21. Требования режима защиты информации в процессе рекламной деятельности.
22. Требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.
23. Задачи, функции и структуру подразделений защиты информации.
24. Принципы, методы и технологию управления подразделений защиты информации.
25. Методы проверки персонала по защите информации;
26. Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.
27. Социально-психологические факторы, влияющие на расстановку кадров.
28. Формы создания и способы поддержания необходимого микроклимата в коллективе.
29. Обеспечение персональной ответственности за сохранность носителей информации.
30. Обеспечение необходимых условий труда.
31. Охрана труда. Культура труда. Карты организации трудового процесса.
32. Понятие и сущность методов управления.
33. Административно-правовые методы управления.

34. Экономические методы управления. Социально-психологические методы управления.
35. Виды планирования, их назначение.
36. Содержание и структура планов.
37. Технология планирования.
38. Методы и формы контроля выполнения планов.
39. Критерии эффективности службы защиты информации.
40. Пути и способы повышения эффективности управления службой защиты информации.
41. Мероприятия по мониторингу направлений деятельности службы защиты информации.
42. Внедрение организационных решений на объектах профессиональной деятельности.
43. Учет, обработка, хранение, передача, использование различных носителей конфиденциальной информации.
44. Техника безопасности при проведении организационно-технических мероприятий.

МДК. 1.3 Организация работы персонала с конфиденциальной информацией

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.Виды и способы охраны объекта.

13.Особенности охраны персонала организации.

14.Основные направления и методы организации режима и охраны объекта.

15.Разрешительная система доступа к конфиденциальной информации.

16.Принципы действия аппаратуры систем контроля доступа.

17.Принципы построения и функционирования биометрических систем безопасности.

18.Требования и особенности оборудования режимных помещений.

19.Требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров.

20.Требования режима защиты информации при приеме в организации посетителей.

21.Организация работы при осуществлении международного сотрудничества.

22.Требования режима защиты информации в процессе рекламной деятельности.

23.Требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.

24.Задачи, функции и структуру подразделений защиты информации.

25.Принципы, методы и технологию управления подразделений защиты информации.

26.Методы проверки персонала по защите информации;

27.Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.

28.Организация работы по защите информации при осуществлении публикаторской деятельности и связей с прессой; участие в ней Службы безопасности

29.Организация контроля за выполнением распорядка дня лицами, работающими на режимных объектах.

30.Создание отдельных (выделенных) производственных зон (зон доступа) по типу и степени конфиденциальности работ с самостоятельными системами организации и контроля доступа.

31.Методика проектирования системы пропускного и внутри объектового режимов и оценки эффективности их функционирования.

32.Организация работы по защите информации при осуществлении публикаторской деятельности и связей с прессой; участие в ней службы безопасности.

33.Методы оценки эффективности защитных мероприятий в рекламной и публикаторской деятельности.

34.Виды и способы охраны. Понятие о рубежах охраны. Много рубежная система охраны.

35.Много рубежная система охраны.

36.Порядок вывоза (выноса) материальных ценностей и документации с территории организации и ввоза (вноса) их на территорию.

37.Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта. Порядок допуска работников в помещения, где ведутся конфиденциальные работы.

38.Методика проектирования системы пропускного и внутри объектового режимов и оценки эффективности их функционирования.

39. Составление списков участников совещания

40. Определение состава информации, используемой в ходе совещаний, переговоров.

41.Организация и проведении проверок объектов информатизации, подлежащих защите.

42.Контроль соблюдения персоналом требований режима защиты информации.

43.Оценка качества защиты объекта.

Оценка индивидуальных образовательных достижений по результатам текущего контроля и промежуточной аттестации производится в соответствии с универсальной шкалой (таблица).

Процент результативности (правильных ответов)	**Качественная оценка индивидуальных образовательных достижений**	
	балл (отметка)	**вербальный аналог**
85 ÷ 100	5	отлично
70 ÷ 84	4	хорошо
50 ÷ 69	3	удовлетворительно
менее 50	2	не удовлетворительно

6.ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В РАБОЧУЮ ПРОГРАММУ

№ изменения, дата изменения; № страницы с изменением	
БЫЛО	**СТАЛО**
Основание: Подпись лица внесшего изменения	