Департамент образования Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

по специальности
10.02.01 Организация и технология защиты информации

квалификация
Техник по защите информации

Белгород 2021 г.

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

Рассмотрено
п р е д м е т н о - ц и к л о в о й комиссией
Протокол заседания № __
От «31» августа 2021 г.
Председатель цикловой комиссии
_____/Алиева Э.Н./

Согласовано
Зам.директора по УМР

_____/ Бакалова Е.Е.
«31» августа 2021 г.

Утверждаю
Заместитель директора по УР

_____/ Выручаева Н.В.
«31» августа 2021 г.

Рассмотрено
п р е д м е т н о - ц и к л о в о й комиссией
Протокол заседания № ___
от «____»_____20__ г.
Председатель цикловой комиссии
_____/_____

Рассмотрено
п р е д м е т н о - ц и к л о в о й комиссией
Протокол заседания № ____
от «____»_____20__ г.
Председатель цикловой комиссии
_____/_____

Рассмотрено
п р е д м е т н о - ц и к л о в о й комиссией
Протокол заседания № ____
От «____»_____20_ г.
Председатель цикловой комиссии
_____/_____

Организация разработчик: ОГАПОУ «Белгородский индустриальный колледж»
Составитель:
преподаватель ОГАПОУ «Белгородский индустриальный колледж»
Солдатенко М.Н.
Экспертиза:
(*внутренний рецензент*) ОГАПОУ «Белгородский индустриальный колледж», преподаватель, Внукова Н.В.
(*внешний рецензент*) ООО «Фортуна», генеральный директор, Мочалов В.И.

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 рабочая программа) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО **10.02.01«Организация и технология защиты информации»** (базовой подготовки), входящей в укрупненную группы специальностей 10.00.00 «Информационная безопасность», в части освоения основного вида профессиональной деятельности (ВПД): Планирование и организация работ по обеспечению защиты объекта и соответствующих профессиональных компетенций (ПК):

ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.

ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.

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

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

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

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

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

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

ПК 1.9. Участвовать в оценке качества защиты объекта.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке по направлению 10.02.01«Организация и технология защиты информации» при наличии среднего (полного) общего образования. Опыт работы не требуется.

Код по Общероссийскому классификатору профессий рабочих, должностей служащих и тарифных разрядов (ОК 016-94)	**Наименование профессий рабочих, должностей служащих**
16199	Оператор электронно-вычислительных и вычислительных машин
21299	Делопроизводитель

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

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- использования физических средств защиты объекта;
- применения физических средств контроля доступа на объект;
- ведения текущей работы исполнителей с конфиденциальной информацией;

уметь:

- организовывать охрану персонала, территорий, зданий, помещений и продукции организаций; пользоваться аппаратурой систем контроля доступа;
- выделять зоны доступа по типу и степени конфиденциальности работ;
- определять порядок организации и проведения рабочих совещаний;
- использовать методы защиты информации в рекламной и выставочной деятельности; использовать критерии подбора и расстановки сотрудников подразделений защиты информации;
- организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
- проводить инструктаж персонала по организации работы с конфиденциальной информацией;
- контролировать соблюдение персоналом требований режима защиты информации.

знать:

- виды и способы охраны объекта;
- особенности охраны персонала организации;
- основные направления и методы организации режима и охраны объекта;
- разрешительную систему доступа к конфиденциальной информации;
- принципы действия аппаратуры систем контроля доступа;
- принципы построения и функционирования биометрических систем безопасности;
- требования и особенности оборудования режимных помещений;
- требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров;
- требования режима защиты информации при приеме в организации посетителей;
- организацию работы при осуществлении международного сотрудничества;
- требования режима защиты информации в процессе рекламной деятельности;
- требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;
- задачи, функции и структуру подразделений защиты информации;
- принципы, методы и технологию управления подразделений защиты информации;
- порядок оформления допуска лиц к конфиденциальным сведениям;
- методы проверки персонала по защите информации;

- процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – **858 часов**, в том числе:
максимальной учебной нагрузки обучающегося – **534 часов**, включая:
обязательной аудиторной учебной нагрузки обучающегося – **356 часов**;
самостоятельной работы обучающегося – **178 часов**,
в том числе консультаций – **55 часов**;
учебной практики – **180 часов**;
производственной практики – **144 часа**.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) **Участие в планировании и организации работ по обеспечению защиты объекта**, в том числе профессиональными(ПК)и общими(ОК)компетенциями:

Код	Наименование результата обучения
ПК 1.1	Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации
ПК 1.2	Участвовать в разработке программ и методик организации защиты информации на объекте
ПК 1.3	Осуществлять планирование и организацию выполнения мероприятий по защите информации
ПК 1.4	Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности
ПК 1.5	Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации
ПК 1.6	Обеспечивать технику безопасности при проведении организационно-технических мероприятий
ПК 1.7	Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите
ПК 1.8	Проводить контроль соблюдения персоналом требований режима защиты информации
ПК 1.9	Участвовать в оценке качества защиты объекта
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного

	развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10	Применять математический аппарат для решения профессиональных задач.
ОК 11	Оценивать значимость документов, применяемых в профессиональной деятельности.
ОК12	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профессиональных компетенций	**Наименования разделов профессионального модуля***	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов
			Всего, часов	**в т.ч. практические занятия, семинары** часов	**в т.ч., курсовая работа (проект),** часов	**Всего,** часов	**в т.ч., консультации,** часов		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
ПК 1.1-1.9	**Раздел 1.** Организация системы безопасности организации	**240**	**160**	46	40	**80**	27		
ПК 1.1-1.9	**Раздел 2.** Организация и управление подразделений защиты информации	**156**	**104**	50		**52**	14		
ПК 1.1-1.9	**Раздел 3.** Работа персонала с конфиденциальной информацией	**138**	**92**	30		**46**	14		
	Учебная практика	**180**						**180**	
	Производственная практика	**144**							**144**
	Всего:	**858**	**356**	126	40	**178**	55	**180**	**144**

*Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

3.2 Содержания обучения по профессиональному модулю (ПМ)
ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)		Объем часов	Уровень освоения
1	**2**		**3**	**4**
Раздел 1. Организация системы безопасности организации			**240**	
МДК 01.01. Обеспечение организации системы безопасности предприятия			**240**	
Тема 1.1. Сущность и задачи комплексной защиты информации организации	**Содержание**		**10**	2
	1	Предмет, цели и задачи и содержание междисциплинарного курса .Структура МДК. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия .Понятийный аппарат в области обеспечения безопасности информации. Общие понятия информации, безопасности информации, защиты информации и конечных целей защиты. Цели, задачи и принципы построения комплексной системы защиты информации. Понятие целей и задач КСЗИ. Принципы КСЗИ. Принцип системности. Принцип комплексности. Принцип своевременности. Принцип непрерывности. Принцип разумной достаточности. Принцип простоты применения.	
	2	Разумная достаточность и экономическая эффективность. Принцип разумной достаточности защиты информации организации. Сохранение состояния адекватности организации. Зависимость состояния защищенности от уровня экономического развития организации. Обоснование экономической эффективности КСЗИ.	
	3	Управление безопасностью организации. Международные стандарты. Разработка концепции управления безопасности предприятием, как фактор, влияющий на построение КСЗИ. Основные положения российских стандартов по	

		информационной безопасности. Стандарты, разработанные комитетом ISO/IECJTC 1/SC27. ГОСТ РИСО/МЭК.		
	4	Цели и задачи защиты информации в автоматизированных системах. Этапы защиты информации в АС. Системно-концептуальный подход к защите информации в АС. Требования к комплексной системе защиты информации в АС. Основные цели и задачи, которые должна решать система защиты информации в АС		
	5	Современное понимание методологии защиты информации. Особенности национального технического регулирования. Что понимается под безопасностью информационных технологий? Документы пользователя. Требования к средствам обеспечения безопасности.		
Тема 1.2. Принципы организации и этапы разработки комплексной защиты информации (КСЗИ.)	**Содержание**		**10**	2
	1	Методологические основы организации КСЗИ. Направления работ по созданию КСЗИ. Комплексные задачи, решаемые методологическим аппаратом.		
	2	Разработка политики безопасности и регламента безопасности организации. Планирование безопасности организации. Политика безопасности, как документ верхнего уровня. Соблюдение принципа разумной достаточности. Регламент безопасности, как документ, регламентирующий правила обращения с конфиденциальной информацией в зависимости от фазы ее обработки и категории конфиденциальности		
	3	Основные положения теории сложных систем. Базовые понятия теории систем: операция; цель операции; система; задача системы; стратегия; операционная система; операционный комплекс.		
	4	Система управления информационной безопасностью организации. Принципы построения и взаимодействие с другими подразделениями. Состав системы управления информационной безопасностью организации (СУИБ). Структура системы управления безопасностью информации и отдела обеспечения безопасности информации. Основные направления деятельности СУИБ.		
	5	Требования, предъявляемые к КСЗИ. Требования к организационной и технической составляющим КСЗИ. Требования по безопасности, предъявляемые к изделиям ИТ: порядок задания требований, разработка изделия ИТ, обеспечение поддержки доверия к безопасности изделия ИТ		

		при эксплуатации, Подтверждение соответствия изделий ИТ требованиям безопасности информации, поставка и ввод в действие, эксплуатация объекта.		
	Практические занятия		**2**	
	1	Изучение этапов разработки КСЗИ.		
Тема 1.3. Факторы, влияющие на организацию комплексной системы защиты информации	**Содержание**		**8**	2
	1	Влияние формы собственности на особенности защиты информации ограниченного доступа. Российская собственность. Иностранная собственность. Совместная российская и иностранная собственность. Смешанная российская собственность с долей государственной собственности.		
	2	Характер основной деятельности предприятия. Классификация предприятий по виду деятельности. Специфические особенности КСЗИ организации, связанные с организацией и проведением организационных, правовых и технических мероприятий защиты информации.		
	3	Состав, объекты и степень конфиденциальности защищаемой информации. Основные особенности защиты информации в зависимости от состава защищаемой информации: государственная тайна, служебная тайна, коммерческая тайна, персональные данные.		
	4	Структура и территориальное расположение организации. Классификация предприятий по их структуре, влияющая на определение параметров КСЗИ. Территориальное расположение предприятий, как условие функционирования КСЗИ.		
	Практические занятия		**4**	
	2	Конструктивные особенности организации, как фактор влияющий на КСЗИ		
	3	Количественные и качественные показатели ресурсообеспечения, как факторы влияющие на КСЗИ. Степень автоматизации основных процедур обработки защищаемой информации		
Тема 1.4. Определение и нормативное закрепление	**Содержание**		**2**	2
	1	Классификация информации по видам тайны и степеням конфиденциальности Нормативно-правовые аспекты определения состава защищаемой информации.		

		Задачи, влияющие на определение состава защищаемой информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия.		
	Практические занятия		**2**	
	4	Методика определения состава защищаемой информации.		
Тема 1.5. Определение объектов защиты.	**Содержание**		**6**	2
	1	Значение носителей защищаемой информации как объектов защиты. Носители информации как объект правовых отношений. Носители информации как возможный источник ее утечки. Особенности помещений как объектов защиты для работы по защите информации.		
	2	Факторы, определяющие необходимость защиты периметра и здания предприятия. Злоумышленник не ограничен в выборе объекта несанкционированного доступа. Злоумышленник не ограничен в выборе момента и продолжительности несанкционированного доступа. Злоумышленник не ограничен в выборе средств, способов и методов несанкционированных действий.		
	3	Требования к помещениям для работы с защищаемой информацией. Нормативные и методические документы, устанавливающие требования к помещениям, предназначеным для работы с информацией ограниченного доступа. Основные принципы оборудования сигнализацией помещений. Сейфы и хранилища ценностей		
	Практические занятия		**8**	
	5	Изучение методики выявления состава носителей защищаемой информации.		
	6	Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа		
	7	Транспортные средства и особенности транспортировки, как объект защиты информации организации.		
	8	Изучение состава средств обеспечения, подлежащих защите		
Тема 1.6. Дестабилизирующие воздействия на информацию и их нейтрализация	**Содержание**		**4**	2
	1	Факторы, создающие угрозу информационной безопасности. Количественная недостаточность системы защиты. Качественная недостаточность системы защиты. Отказы. Сбои. Ошибки операторов АС. Стихийные бедствия. Злоумышленные действия. Побочные явления. Объективные и субъективные		

		факторы.		
	2	Угрозы безопасности информации. Обеспечение безопасности информации в непредвиденных ситуациях. План действий в непредвиденных ситуациях. Проведение обучения по действиям в непредвиденных ситуациях. Выделение мест резервного хранения информации. Резервирование телекоммуникационных услуг. Разработка требований по восстановлению ИТ		
	Практические занятия		**6**	
	9	Модели нарушителей безопасности автоматизированных систем.		
	10	Подходы к оценке ущерба от нарушений информационной безопасности		
	11	Резервирование информации и отказоустойчивость		
Тема 1.7. Определение возможностей несанкционированного доступа к защищаемой информации.	**Содержание**		**2**	3
	1	Методы и способы защиты информации. Классификация средств защиты информации НСД. Методы защиты данных: препятствия, маскировка, регламентация, побуждение, принуждение. Формальные и неформальны средства защиты данных. Классификация СЗИ. НСД: по месту применения, по объектам защиты отдельного компьютера, по функциональному назначению. Механизмы обеспечения безопасности информации		
	Практические занятия		**4**	
	12	Средства защиты информации в локальных сетях. Средства защиты доступа к компьютеру		
	13	Методика выявления нарушителей, тактики их действий и состава интересующей их информации		
Тема 1.8. Определение компонентов комплексной системы защиты информации организации	**Содержание**		**2**	2
	1	Особенности синтеза СЗИ автоматизированных систем от НСД. Методика синтеза средств защиты информации. Выбор структуры СЗИ автоматизированной системы. Общее описание архитектуры автоматизированных систем, системы защиты информации и политики безопасности. Формализация описания архитектуры исследуемой автоматизируемой системы. Формулирование требований к системе защиты информации. Выбор механизмов и средств защиты информации. Определение		

		важности параметров средств защиты информации. Линейная, кольцевая, сотовая, многосвязная и звездная структуры СЗИ АС.		
	Практические занятия		**2**	
	14	Проектирование системы зашиты информации для существующей автоматизированной системы		
Тема 1.9. Определение условий функционирования комплексной системы защиты информации организации	**Содержание**		**2**	3
	1	Содержание концепции построения КСЗИ. Объекты защиты. Цели и задачи обеспечения безопасности информации. Основные угрозы безопасности АС организации. Основные положения технической политики в области обеспечения безопасности информации АС организации. Основные принципы построения КСЗИ. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Первоочередные мероприятия по обеспечению безопасности информации АС организации		
	Практические занятия		**4**	
	15	Управление системой обеспечения безопасности информации в АС		
	16	Контроль эффективности защиты информации		
Тема 1.10. Разработка модели комплексной системы защиты информации организации	**Содержание**		**2**	3
	1	Общая характеристика задач моделирования КСЗИ. Формальные модели безопасности. Прикладные модели защиты информации в АС. Этапы процесса моделирования. Основные задачи моделирования. Понятие и классификация формальных и прикладных моделей защиты информации в АС.		
	Практические занятия		**2**	
	17	Модели обеспечения конфиденциальности и целостности. Формальное построение модели защиты		
Тема 1.11. Технологическое и организационное построение комплексной системы защиты информации организации	**Содержание**		**4**	2
	1	Характеристика основных стадий создания КСЗИ. Назначение и структура технического задания. Организационное направление работ по созданию КСЗИ. Техническое направление работ по созданию КСЗИ. Общие требования к содержанию технического задания.		

	2	Предпроектное обследование, рабочий проект. Апробация и ввод в эксплуатацию		
Тема 1.12. Кадровое обеспечение функционирования комплексной системы защиты информации	**Содержание**		**4**	3
	1	Специфика персонала предприятия как объекта защиты. Подбор и расстановка кадров. Юридическое обеспечение. Изучение персонала службой безопасности. Обучение персонала. Ротация кадров. Безопасность персонала.		
	2	Распределение функций по защите информации. Функции руководства предприятия. Функции службы защиты информации. Функции специальных комиссий. Обязанности пользователей защищаемой информации		
	Практические занятия		**2**	
	18	Подбор персонала. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа.		
Тема 1.13. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации	**Содержание**		**4**	3
	1	Состав и значение материально-технического обеспечения функционирования КСЗИ. Объекты хозяйственного и технического значения материально технической базы КСЗИ. Состав материально-технического обеспечения КСЗИ.		
	2	Перечень вопросов защиты информации, требующих документационного закрепления. Комплект внутренних нормативных и методических документов. Инструкция по защите от несанкционированного доступа. Положение о категорировании ресурсов. Положение об отделе технической защиты информации. Обязанности администратора информационной безопасности Подразделения. Инструкция по организации парольной защиты		
	Практические занятия		**4**	
	19	Материальные средства системы защиты информации		
	20	Порядок обращения с информацией, подлежащей защите		
Тема 1.14. Сущность и содержание контроля функционирования комплексной системы защиты информации	**Содержание**		**4**	3
	1	Виды контроля функционирования КСЗИ. Цель проведения контрольных мероприятий в КСЗИ. Основные требования к контролю. Общие цели контроля. Современные виды контроля. Внешний и внутренний контроль. Основные задачи контроля. Направления		

организации		контроля состояния защиты информации. Принципы системы контроля состояния защиты информации. Функции органа контроля. Анализ и использование результатов проведения контрольных мероприятий.		
	2	Периодичность проведения проверок технической защиты информации. Нарушения в области технической защиты информации. Содержание контроля состояния технической защиты информации. Контроль деятельности по технической защите информации. Контроль эффективности защиты.		
	Практические занятия		**2**	
	21	Контроль КСЗИ в информационных и автоматизированных системах обработки информации		
Тема 1.15. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций	**Содержание**		**2**	2
	1	Понятие и основные виды чрезвычайных ситуаций в организации. Технология принятия решений в условиях чрезвычайных ситуаций Факторы, влияющие на принятие решений в условиях чрезвычайных ситуаций. Практические действий работников при чрезвычайных ситуациях		
Тема 1.16. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации организации	**Содержание**		**6**	3
	1	Вероятностный подход. Аналитические методы. Численные методы. Методы статистических испытаний. Методы статистического имитационного моделирования. Метод вероятностной скаляризации Оценочный подход. Основополагающие оценочного подхода к оценке эффективности КСЗИ, Группы требований по защите конфиденциальной информации по характеру их детализации.		
	2	Требования РД средств вычислительной техники и РД автоматизированных систем. Классы защищенности средств вычислительной техники от НСД к информации. Классы защищенности АС от НСД к информации. Основные требования руководящих документов.		
	3	Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408—2002. Экспериментальный подход. Концепция аудита информационной безопасности систем информационных технологий и организаций. Виды аудита информационной безопасности. Формы аудита ИБ		

	Практические занятия		**4**	
	22	Аналитические методы оценки эффективности функционирования сложных информационных систем		
	23	Аудиторская организация по ИБ		
Тема 1.17. Методы и модели оценки эффективности комплексной системы защиты информации	**Содержание**		**2**	2
		Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Экономический подход к оценке эффективности КСЗИ. Метод относительного ранжирования. Личный опрос. Заочный опрос. Групповые методы опроса. Метод комиссии. Метод суда. Метод мозговой атаки. Синектика. Метод Дельфы. Определение размеров ущерба с использованием моделей «осведомленность —эффективность. Определение размеров ущерба с использованием экспертных оценок. Определение затрат на защиту информации		
Самостоятельная работа обучающихся по разделу 1 (в том числе консультации) 1 Понятия безопасности и защищенности (презентация). 2 Этапы защиты информации в АС (презентация). 3 Разграничение зоны ответственности между службой безопасности и IT-службой предприятия (схема). 4 Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа (доклад) 5 Зависимость КСЗИ от классификации организаций по типу производственной кооперации (презентация). 6 Государственная, служебная и коммерческая тайны (сравнительная характеристика). 7 Режим функционирования организации, как фактор влияющий на организацию КСЗИ (презентация). 8 Порядок внедрения Перечня сведений, составляющих коммерческую тайну, внесение в него изменений и дополнений (презентация). 9 Основные источники защищаемой информации (таблица). 10 Категории доступа помещений предприятия для работы с защищаемой информацией (презентация). 11 Объективные и субъективные факторы, создающие угрозу информационной безопасности (схема). 12 Виды угроз, приведенные в Приложении 2 к «Руководству по разработке профилей защиты и заданий по безопасности», выпущенном ФСТЭК России в развитии ГОСТ 15408—2002 (схема). 13 Разработка требований к резервному копированию информации (презентация). 14 Описание каналов утечки информации (сводная таблица) 15 Задачи КСЗИ по выявлению угроз и каналов утечки информации (структурная схема). 16 Классификация методов и средств защиты данных (обобщающая схема) 17 Элементы систем аутенфикации (таблица). 18 Типы межсетевых экранов (презентация)			**80** (27)	

19 Структуры СЗИ автоматизированной системы (сравнение) 20 Угрозы по безопасности АС и меры по их нейтрализации (презентация) 21 Анализ формальных моделей безопасности. 22 Общее содержание работ по организации КСЗИ (презентация). 23 Технический проект КСЗИ (реферат). 24 Основные направления развития и совершенствования МТО ЗИ (презентация). 25 План обеспечения непрерывной работы и восстановления. 26 Перечень внутренних организационно-распорядительных документов для объекта ВТ (презентация). 27 Принципы управления КСЗИ: комплексность, своевременность, непрерывность, активность, законность, обоснованность, специализация, взаимодействие и координация, централизация управления (сравнительный анализ). 28 Основные стили управления (презентация). 29 Факторы, влияющие на выбор способов планирования (презентация). 30 Общая типовая схема решения задач оперативного управления в КСЗИ. 31 Основные методы контроля, виды контроля эффективности защиты (реферат). 32 Методы оценки эффективности сложных информационных систем (схема) 33 Показатели защищенности по классам СВТ (таблица) 34 Определение упущенной выгоды в результате ограничений на распространение информации (реферат).		
Обязательная аудиторная учебная нагрузка обучающегося по курсовой работе (проекту)	**40**	
Тематика курсовых работ (проектов) 1. Построение концепции информационной безопасности предприятия (название предприятия) 2. Разработка комплексной системы защиты информации (КСЗИ) предприятия (название предприятия) 3. Организация безопасного удаленного доступа к ЛВС предприятия (название предприятия) 4. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (название предприятия). 5. Организация процессов мониторинга конфиденциального документооборота на предприятии (название предприятия) 6. Автоматизация процесса проверок наличия конфиденциальных документов на предприятии (название предприятия) 7. Организация системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия) 8. Разработка основных направлений совершенствования КСЗИ предприятия (наименование предприятия) 9. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия) 10. Разработка методологии проектирования КСЗИ 11. Разработка моделей процессов защиты информации при проектировании КСЗИ 12. Анализ методов оценки качества функционирования КСЗИ 13. Разработка структурно-функциональной модели управления КСЗИ предприятия (наименование предприятия) 14. Разработка проекта программно-аппаратной защиты информации предприятия (наименование предприятия)		

15. Разработка методов расчета экономической эффективности программно-аппаратной защиты информации предприятия (наименование предприятия) 16. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия) 17. Анализ нормативно-правовой базы по защите информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет (название предприятия) 18. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия) 19. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия) 20. Организация порядка установления внутриобъектного спецрежима на объекте информатизации (название предприятия) 21. Использование институтов правовой защиты интеллектуальной собственности для защиты информации (название объекта) 22. Организация защиты персональных данных на основе использования правовых мер (название предприятия) 23. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну (название предприятия) 24. Разработка и анализ эффективности внедрения мер по защите информации торговых автоматов, подключенных к глобальной сети и управляемых удаленно (название предприятия) 25. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия) 26. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия). 27. Разработка систем видеонаблюдения и сигнализации для обеспечения защиты информации в (название предприятия). 28. Организация автоматизированного пропускного режима на крупном предприятии (на примере). 29. Разработка проекта организационных мер по защите аудиоинформации в локальной сети (название предприятия). 30. Разработка комплексной системы защиты информации в кабинете директора (название предприятия). 31. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии . 32. Разработка системы защиты информации конфиденциального характера от утечки по техническим каналам в (название предприятия). 33. Разработка организационного порядка установления внутриобъектного режима для торговой фирмы (название предприятия). 34. Организация системы контроля доступа и защиты информации на предприятии (название предприятия) 35. Разработка комплексной системы защиты информации в кабинете руководителя предприятия		

36. Защита речевой информации в каналах связи коммерческих организаций. 37. Разработка проекта корпоративной сети (название предприятия) 38. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия) 39. Разработка мероприятий организационного характера по обеспечению комплексной защиты информации для (название предприятия) 40. Разработка систем видеонаблюдения и контроля доступа к объектам информатизации в (название предприятия).				
Раздел 2. Работа подразделений защиты информации			**156**	
МДК 01.02. Организация работ подразделений защиты информации			**156**	
Введение		Предмет, цели, задачи и содержание междисциплинарного курса Значение и место курса в подготовке кадров по специальности «Организация и технология защиты информации». Структура МДК. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.	**2**	1
Тема 2.1. Место и роль подразделений защиты информации в системе защиты информации	**Содержание**		**6**	2
	1	Назначение подразделений защиты информации. Место подразделений защиты ин- формации в системе безопасности предприятия.	**4**	
	2	Подразделения защиты информации как составная часть системы защиты и как орган управления защитой информации.		
	Практические занятия		**2**	
	1	Служба защиты информации как координатор деятельности по обеспечению безопасности информации		
Тема 2.2. Задачи и функции подразделений защиты информации	**Содержание**		**14**	2
	1	Организационные задачи и функции подразделений зашиты информации.	**10**	
	2	Технологические задачи и функции подразделений защиты информации.		

	3	Координационные задачи и функции подразделений защиты информации.		
	Практические занятия		**4**	
	2	Взаимосвязь и соотношение организационных, технологических и координационных задач и функций		
	3	Факторы, влияющие на определение задач и функций службы защиты информации.		
Тема 2.3. Структура и штаты подразделений защиты информации	**Содержание**		**12**	2
	1	Общая структурная схема подразделений защиты информации. Факторы, определяющие конкретную структуру подразделений защиты информации.	**4**	
	2	Виды и типы организационных структур подразделений защиты информации. Централизованная и децентрализованная структуры подразделений защиты информации, условия, критерии, определяющие выбор структур.		
	Практические занятия		**8**	
	4	Должностной состав сотрудников подразделений защиты информации, его зависимость от характера выполняемых работ		
		Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений защиты информации		
	6	Функции сотрудников и уполномоченных подразделений защиты информации		
	7	Факторы, определяющие численность сотрудников подразделений защиты информации.		
Тема 2.4. Организационные основы и принципы деятельности подразделений защиты информации	**Содержание**		**8**	2
	1	Порядок создания подразделений защиты информации. Структура и содержание положения о подразделениях защиты информации. Состав и содержание других нормативных документов, регламентирующих деятельность подразделений защиты информации.	**4**	
	2	Основные принципы организации и деятельности подразделений защиты информации.		

	Практические занятия		**4**	
	8	Условия и факторы, влияющие на организацию работы подразделений защиты информации		
	9	Организация взаимодействия службы защиты информации и подразделений предприятия		
Тема 2.5. Подбор, расстановка и обучение сотрудников подразделений защиты информации	**Содержание**		**10**	2
	1	Общие требования, предъявляемые к сотрудникам подразделений защиты информации. Особенности подбора кадров.	**4**	
	2	Формы создания и способы поддержания необходимого микроклимата в коллективе.		
	Практические занятия		**6**	
	10	Формы повышения квалификации сотрудников.		
	11	Методы получения информации о кандидатурах на должности.		
	12	Социально-психологические факторы, влияющие на расстановку кадров.		
Тема 2.6. Организация труда сотрудников подразделений защиты информации	**Содержание**		**16**	2
	1	Деятельность сотрудников подразделений защиты информации. Обеспечение персональной ответственности за сохранность носителей информации.	**10**	
	2	Структура и содержание должностных инструкций сотрудников подразделений защиты информации		
	3	Организация рабочих мест сотрудников подразделений зашиты информации (рациональное размещение, оснащение оборудованием, техническими средствами).		
	Практические занятия		**6**	
	13	Обеспечение необходимых условий труда. Охрана труда. Карты организации трудового процесса.		
	14	Специфика деятельности сотрудников службы защиты информации.		
	15	Распределение обязанностей между сотрудниками подразделений защиты информации.		

Тема 2.7. Принципы и методы управления подразделений защиты информации	**Содержание**		**18**	2
	1	Принципы управления подразделениями защиты информации. Понятие и сущность методов управления. Система методов управления.	**12**	
	2	Административно-правовые методы управления.		
	3	Экономические методы управления.		
	4	Социально-психологические методы управления.		
	Практические занятия		**6**	
	16	Принципы и методы управления подразделений		
	17	Взаимосвязь методов управления.		
	18	Необходимость комплексного и системного применения методов управления службой защиты информации.		
Тема2.8. Технология управления подразделениями защиты информации	**Содержание**		**18**	3
	1	Состав управленческих функций. Содержание управленческих функций. Технология управления подразделениями защиты информации. Значение управленческих решений	**4**	
	2	Цели планирования. Виды планирования, их назначение. Содержание и структура планов. Технология планирования. Методы и формы контроля выполнения планов		
	Практические занятия		**14**	
	19	Основные функции службы безопасности		
	20	Организация службы безопасности		
	21	Разведывательное подразделение		
	22	Контрразведывательное подразделение		
	23	Критерии эффективности службы защиты информации		
	24	Методы оценки качества службы защиты информации.		
	25	Пути и способы повышения эффективности управления службой защиты		

		информации.		
Самостоятельная работа обучающихся по разделу 2 (в том числе консультации) 1. Статус подразделения защиты информации в структуре предприятия (доклад). 2. Организационные, технологические и координационные задачи и функции (сравнительный анализ). 3. Виды организационных структур подразделений защиты информации (презентация). 4. Ответственность заместителя руководителя предприятия по безопасности в области защиты информации (доклад). 5. Условия и факторы, влияющие на организацию работы подразделений защиты информации (презентация) 6. Специфические требования, предъявляемые к сотрудникам службы защиты информации (презентация) 7. Подготовка кадрового резерва (доклад) 8. Методика определения численного состава подразделений защиты информации (сообщение) 9. Культура труда (презентация). 10. Особенности приема сотрудников в подразделения защиты информации (презентация) 11. Особенности увольнения сотрудников подразделения защиты информации (презентация). 12. Общие принципы управления подразделениями защиты информации (сравнительный анализ) 13. Методы управления подразделениями защиты информации (сравнительный анализ) 14. Управленческие функции (презентация)			**52** (18)	
Раздел 3. Работа персонала с конфиденциальной информацией			**138**	
МДК 01.03. Организация работы персонала с конфиденциальной информацией			**138**	
Введение	1	Предмет, цели, задачи и содержание междисциплинарного курса Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.	**2**	1
	2	Предпосылки и направления совершенствования технологии защиты и обработки конфиденциальных документов в условиях развития научно-технического прогресса и рыночных экономических отношений.	**6**	
	3	Методика работы над проблемами курса. Обзор изучаемых источников и литературы. Законодательные акты. Нормативные документы.		
	4	Инструкции, методические указания и правила.		
Тема 3.2. Особенности	**Содержание**		**6**	

работы с персоналом, владеющим конфиденциальной информацией	1	Особенности подбора персонала для работы с конфиденциальной информацией.		
	2	Угрозы безопасности информации от персонала и направления ее защиты.		
	3	Психологические особенности личности человека, владеющего тайной.		
	Практические занятия		**4**	
	1	Подбор персонала для работы с конфиденциальной информацией		
	2	Персонал как основная опасность утраты конфиденциальной информации		
Тема 3.3. Задачи и стадии работы с персоналом, обладающим конфиденциальными сведениями.	**Содержание**		**6**	**2**
	1	Особенности приема (перевода) сотрудников на работу, связанную с владением конфиденциальной информацией.		
	2	Принципы подбора персонала. Технологическая цепочка - этапы, процедуры и методы подбора.		
	3	Состав документов, получаемых от кандидата на должность, анализ документов.		
	Практические занятия		**4**	
	3	Методы получения конфиденциальной информации у персонала.		
	4	Составление договора при приеме сотрудников на работу связанную с владением конфиденциальной информацией.		
Тема 3.4. Особенности проведения собеседования, анкетирования, тестирования и опроса.	**Содержание**		**8**	
	1	Критерии отбора кандидатов на должность.		
	2	Особенности документирования приема или перевода на должность.		
	3	Формы обязательств о неразглашении тайны		
	4	Особенности содержательной части контракта		
	Практические занятия		**4**	
	5	Составление анкеты, тестов, схемы опроса для отбора кандидатов на должность, связанную с конфиденциальной информацией.		
	6	Разработка формы обязательств о неразглашении тайны		

Тема 3.5. Доступ персонала к конфиденциальным сведениям, документам и базам данных.	**Содержание**		**4**
	1	Цели и задачи разрешительной (разграничительной) системы доступа персонала и иных лиц к конфиденциальным сведениям, документам, базам данных и продукции.	
	2	Структура разрешительной системы и ее связь с требованиями деловой целесообразности и персональной ответственности руководителей и сотрудников за сохранность тайны фирмы.	
	Практические занятия		**4**
	7	Оформление разрешения о допуске сотрудника к конфиденциальным сведениям. Ответственность должностного лица за выданное разрешение. Понятие доступа	
	8	Принципы построения разрешительной системы доступа, разграничение прав доступа к засекреченной информации	
Тема3. 6. Иерархичность процедуры доступа персонала, обладающего конфиденциальной информацией.	**Содержание**		**10**
	1	Принципы разграничения выдачи разрешения на доступ и непосредственного доступа к информации.	
	2	Методы расчленения (дробления) ценных сведений. Критерии доступа.	
	3	Формы письменной индивидуальной регламентации разрешения на доступ - резолюции, перечни, списки, матрицы, схемы и т. п.	
	4	Обязанности руководителей. Контроль за доступом.	
	5	Регистрация (протоколирование) фактов доступа. Несанкционированный доступ.	
	Практические занятия		**4**
	9	Порядок доступа к конфиденциальным сведениям представителей других фирм и служащих государственных учреждений.	
	10	Создание письменной регламентации разрешения на доступ	
Тема 3.7. Работы с персоналом, обладающим конфиденциальной информацией.	**Содержание**		**6**
	1	Классификация сотрудников по степени их владения тайной фирмы и объемам известной им конфиденциальной информации.	
	2	Направления и методы работы с каждой из выделенных категорий.	

	3	Принципы, организационные формы и методика обучения сотрудников правилам обеспечения безопасности информации.		
	Практические занятия		**4**	
	11	Профессиональная тайна		
	12	Информация ограниченного доступа		
Тема 3.8. Периодическое инструктирование сотрудников, формы проведения, методика.	**Содержание**		**8**	**3**
	1	Формы и методы индивидуальной работы с сотрудниками. Анкетирование, тестирование		
	2	Порядок обучения сотрудников правилам поведения в различных экстремальных ситуациях.		
	3	Методы контроля соблюдения персоналом правил работы с конфиденциальной информацией.		
	4	Порядок проведения служебного расследования по фактам разглашения или утечки конфиденциальной информации, утраты документов и носителей информации.		
	Практические занятия		**4**	
	13	Создание инструкции по соблюдению персоналом правил работы с конфиденциальной информацией		
	14	Служебное расследование по фактам разглашения или утечки конфиденциальной информации		
Тема 3.9. Принципы и формы морального и материального стимулирования ответственного отношения сотрудников к работе с конфиденциальной информацией.	**Содержание**		**6**	**2**
	1	Роль психологического климата в воспитании фирменной гордости сотрудников и ответственного отношения к сохранению тайны фирмы.		
	2	Правовая ответственность персонала за разглашение конфиденциальной информации фирмы.		
	3	Особенности увольнения сотрудников с работы. Технологическая цепочка - этапы и процедуры увольнения. Особенности документирования увольнения.		
	Практические занятия		**2**	
	15	Оформление документации при увольнении сотрудников связанных с		

конфиденциальной информации	
Самостоятельная работа обучающихся по разделу 3 (в том числе консультации):	**46**
1. Классификация конфиденциальных документов	(14)
2. Типология персонала в контексте социальной среды	
3. Методики подбора персонала при приеме на работу	
4. Регламент подготовки превентивных мероприятий	
5. Составление докладных записок, актов и справок содержащих конфиденциальную информацию	
6. Применение критериев при обработке внутриорганизационной документации конфиденциального характера	
7. Методики собеседования	
8. Анализ контента сотрудников	
Учебная практика по модулю:	**180**
Виды работ:	
1.Изучение организации охраны персонала, территорий, зданий, помещений и продукции предприятий;	
2.Изучение техники использования аппаратной системы контроля доступа;	
3.Изучение способов выделения зон доступа по типу и степени конфиденциальности работ;	
4.Определение порядка организации и проведения рабочих совещаний;	
5.Изучение использования методов защиты информации в рекламной и выставочной деятельности;	
6.Изучение и использование критериев подбора и расстановки сотрудников подразделений защиты информации;	
7.Изучение организации работы с персоналом, имеющим доступ к конфиденциальной информации;	
8.Изучение порядка проведения инструктажа персонала по организации работы с конфиденциальной информацией.	
9.Изучение процесса контроля соблюдения персоналом требований режима защиты информации	
Производственная практика по модулю:	**144**
Виды работ:	
1. Ознакомление с правилами техники безопасности при работе с ПК и оргтехникой на предприятии, положением о защите информации на предприятии.	
2. Изучение состава, структуры программного обеспечения.	
3. Определение программы и программного обеспечения.	
4. Понятие о лицензионном и нелицензионном программном обеспечении.	
5. Механизмы обеспечения безопасности информации.	
6. Идентификация и аутентификация.	
7. Разграничение доступа, регистрация и аудит.	
8. Межсетевое экранирование.	
9. Организационные задачи и функции подразделений зашиты информации.	
10. Общая структурная схема подразделений защиты информации.	

11. Виды и типы организационных структур подразделений защиты информации.
12. Должностной состав сотрудников подразделений защиты информации.
13. Сбор информации о количестве и состоянии объектов и носителей конфиденциальной информации.
14. Организация и выполнение мероприятий по защите информации и ее носителей.
15. Оценка качества защиты объектов.
16. Проведение проверок объектов информатизации, подлежащих защите, контроль соблюдения персоналом требований режима защиты информации
17. Виды потенциальных угроз безопасности информации
18. Изучение и использование критериев подбора и расстановки сотрудников подразделений защиты информации.
19. Изучение организации работы с персоналом, имеющим доступ к конфиденциальной информации
20. Изучение порядка проведения инструктажа персонала по организации работы с конфиденциальной информацией.
21. Изучение процесса контроля соблюдения персоналом требований режима защиты информации.

Всего: 858

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 программы профессионального модуля предполагает наличие учебного кабинета информационной безопасности, лабораторий технических средств защиты информации; программно-аппаратных средств защиты информации;

Оборудование учебного кабинета и рабочих мест кабинета информационной безопасности:

комплект нормативной документации по организации информационной безопасности; комплект учебно-методической документации; наглядные пособия (плакаты по организации информационной безопасности.

Технические средства обучения: мультимедийное оборудование.

Оборудование лабораторий и рабочих мест лабораторий:

Технические средства защиты информации:

комплект учебно-методической документации; наглядные пособия (плакаты по техническим средствам защиты информации);

компьютеры, маркерная доска, мультимедийный проектор,

программное обеспечение общего и профессионального назначения.

Технические средства обучения:

лабораторное оборудование для технической защиты информации;

мультимедийное оборудование.

Программно-аппаратные средства защиты информации:

комплект учебно-методической документации; наглядные пособия (плакаты по программно-аппаратным средствам защиты информации);

компьютеры, маркерная доска, мультимедийный проектор,

программное обеспечение общего и профессионального назначения.

Реализация программы профессионального модуля предполагает обязательную учебную и производственную практику (по профилю специальности). Учебную и производственную практику (по профилю специальности) рекомендуется проводить концентрированно в специально выделенный период на рабочих местах баз практики.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности [Текст]: учеб. пособие для студентов учреждений среднего проф. образования. - Рек. ФУМО в системе СПО. - М.: Академия, 2017. - 336 с. - (Профессиональное образование) (ТОП-50).

2. Васильева И.Н., Стельмашонок Е.В. Информационные технологии и защита информации. Учебное пособие. – СПб, СПбГИЭУ, 2011
3. Мельников В.П. Информационная безопасность: учебник / под ред., Куприянов А.И. — Москва: КноРус, 2020. — 267 с. — (СПО). — URL: https://book.ru/book/932059 (дата обращения: 30.08.2019). — Текст: электронный.
4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: Форум, Инфра-М, 2015.
4. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии учеб.пособие для студ. высш. учеб. Заведений. — М.: Академия, 2015.

Дополнительные источники:

1. Карпов, В. В. Технология построения защищенных автоматизированных систем : учебное пособие / В. В. Карпов, В. А. Мельник. — М. : Российский новый университет, 2009. — 232 c. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/21326.html (дата обращения: 30.08.2019). — Режим доступа: для авторизир. пользователей\
2. Галатенко В.А. Основы информационной безопасности. — М.: Интуит.Ру, 2005.
3. Степанов Е.А. Защита информации и информационная безопасность. Курс лекций. — М.: Изд-во ГУУ, 2004
4. Шумский А. А., Шелупанов А. А. Системный анализ в защите информации: Учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности. – М.: Гелиос АРВ, 2005.
5. Семкин С. Н., Беляков Э. В., Гребнев С. В., Козачок В. И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие – М.: Гелиос АРВ, 2005.
6. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2004.
7. Дикарев В.И., Заренков В.А., Заренков Д.В., Койнаш Б.В. Защита объектов и информации от несанкционированного доступа/ Под ред. В.А. Заренкова. СПб.: ОАО «Издательство Стройиздат СПб», 2004.
8. Зайцев А.П. Технические средства и методы защиты информации. М.: Горячая линия-Телеком, 2009.
9. Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел: Учебн. пособие/ Под ред. А. А. Чекалина. В 2-х ч. Ч. 1. Теоретические основы технической разведки и комплексного технического контроля. М.:Горячаялиния-Телеком, 2006.с.
10. Меньшаков Ю.К. Виды и средства иностранных технических разведок: Учеб. пособие/ Под ред. М.П. Сычева. М.: Изд-во МГТУ им. Н.Э. Баумана, 2009.

11. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки: Учеб.пособие. М.: Российск. гос. гуманит. ун-т, 2002.
12. Рудометов Е.А., Рудометов В.Е. Электронные средства разведки и защиты информации. М.: ООО «Фирма «Издательство АСТ»; СПб.: ООО «Издательство ПОЛИГОН», 2000.
13. Торокин А. А. Инженерно-техническая защита информации: Учеб.пособие для студентов, обучающихся по специальностям в обл. информ. безопасности. М.: Гелиос АРВ, 2005.
14. Хорев А.А. Техническая защита информации: Учеб.пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008.

Интернет-ресурсы:

1.http://www.pandia.ru/
2.http://www.twirpx.com/
3.http://www.infsec.ru/
4.http://www.booksshare.net/

4.3. Общие требования к организации образовательного процесса

Профессиональный модуль ПМ.01 «Участие в планировании и организации работ по обеспечению защиты объекта» входит в состав профессионального цикла.

Общепрофессиональные дисциплины, изучение которых должно предшествовать освоению данного модуля:

- Документоведение
- Документационное обеспечение управления
- Архивоведение
- Технические средства информатизации
- Базы данных
- Основы информационной безопасности
- Экономика организации
- Организационные основы деятельности организации
- Менеджмент
- Безопасность жизнедеятельности
- Операционные системы
- Компьютерные сети

При освоении профессионального модуля предусматривается использование в образовательном процессе активных и интерактивных форм проведения занятий с применением электронных образовательных ресурсов, деловых игр, индивидуальных и групповых проектов, анализа производственных ситуаций, психологических и иных тренингов, групповых дискуссий в сочетании с внеаудиторной работой для формирования и развития общих и профессиональных компетенций обучающихся. Текущий контроль проводится в форме: устного опроса, защиты практических работ по, выполнения и защиты курсовой работы по МДК.01.01. Освоение каждого

междисциплинарного курса завершается дифференцированным зачетом или экзаменом, а освоение программы профессионального модуля – проведением квалификационного экзамена.

При реализации программы ПМ.01 «Участие в планирование и организации работ по обеспечению защиты объекта» предусматривается производственная практика (по профилю специальности). Производственная практика (по профилю специальности) проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся. Аттестация по итогам производственной практики проводится с учетом (или на основании) результатов, подтвержденных документами соответствующих организаций. Производственная практика (по профилю специальности) завершается зачётом. Освоение междисциплинарного курса заканчивается экзаменом, освоение программы профессионального модуля - проведением экзамена (квалификационного).

Обязательным условием успешного освоения профессионального модуля ПМ.01 «Участие в планировании и организации работ по обеспечению защиты объекта» является обязательное прохождение учебной практики. Учебная практика проводится концентрированно в организациях, направление деятельности которых соответствует профилю подготовки обучающихся. Предусматривается сдача дифференцированного зачета по учебной практике.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): наличие высшего профессионального образования, соответствующего профилю модуля ПМ.01 «Участие в планировании и организации работ по обеспечению защиты объекта» и специальности 10.02.01 «Организация и технология защиты информации».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой

Инженерно-педагогический состав: дипломированные специалисты–преподаватели междисциплинарных курсов.

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

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации	- анализ научной литературы; - правильный выбор решений по обеспечению защиты информации; - выбор методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации; - обоснование выбора соответствующих решений по защите информации объекта; - обоснование использованных методов обнаружения ТКУИ.	Экспертная оценка защиты лабораторных работ Экспертная оценка выполнения практических занятий Компьютерное тестирование по МДК Оценка выполнения самостоятельной работы студентами Экспертная оценка выполнения практического задания по учебной практике Экспертная оценка защиты курсовой работы. Экзамен квалификационный по модулю.
ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте	- умение выработать предложения по разработке программ защиты информации на объекте; - умение самостоятельно разрабатывать методики защиты информации на предприятии.	
ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации	- демонстрация навыков планирования работ по защите конфиденциальной информации; - демонстрация навыков организации мероприятий по комплексной защите информации; - определение качества защиты информации. - обоснование выбранных организационных решений на объектах информатизации; - демонстрация навыков по внедрению организационных решений на предприятии; - умение самостоятельно применять технические средства защиты информации.	

ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности	- правильность использования носителей конфиденциальной информации; - точность соблюдения методики обработки и хранения защищаемой информации; - эффективность и качество выполнения передачи конфиденциальной информации на различных носителях. - полнота и эффективность соблюдения правил использования носителей секретной информации.	
ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации	- демонстрация навыков соблюдения техники безопасности при комплексной защите информации; - умение самостоятельно разрабатывать методики защиты информации при проведении организационно-технических мероприятий.	
ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий	- обоснование выбранных методов проверок организаций, информация которых подлежит защите; - демонстрация навыков по проверок объектов информатизации; - умение самостоятельно проводить проверки организаций, работающих с конфиденциальной информацией.	
ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите	- определение методов и способов контроля персонала, работающего с конфиденциальной информацией; - соблюдение последовательности действий при проведении проверок соблюдения персоналом требований режима защиты информации;	

	- демонстрация навыков проведения контроля за работой персонала, задействованного в защите информации организации.	
ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации	- демонстрация навыков оценки качества комплексной защиты информации организации; - умение самостоятельно оценивать качество защиты объекта информатизации; - определение и анализ недостатков качества защиты информации на предприятии.	
ПК 1.9. Участвовать в оценке качества защиты объекта	- демонстрация навыков оценки качества комплексной защиты информации организации; - умение самостоятельно оценивать качество защиты объекта информатизации.	

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	- участие во внеурочной деятельности, связанной с будущей профессией (конкурсы профессионального мастерства, выставки и т. д.) - высокие показатели производственной деятельности.	Наблюдение за деятельностью обучающихся в процессе освоения образовательной программы: - на практических занятиях, лабораторных работах; - при подготовке рефератов, окладов и т. д.;- при выполнении

безопасности		работ на различных этапах учебной практики
ОК2. 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, оценка их эффективности и качества.	
ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	- решение стандартных и нестандартных профессиональных задач	
ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	- эффективный поиск необходимой информации; использование различных источников, включая электронные при изучении теоретического материала и прохождении различных этапов производственной практики	
ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности	- демонстрация умений использовать информационно-коммуникационные технологии в профессиональной деятельности	

ОК6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения	
ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	- уметь применять средства математической логики для решения задач	
ОК8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	- проявление ответственности за работу подчиненных, результат выполнения заданий	
ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	- организация самостоятельных занятий при изучении профессионального модуля.	
ОК 10. Применять математический аппарат для решения профессиональных задач.	- проявление интереса к новейшим технологиям в области защиты информации.	
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.	- уметь оценивать документы, используемые в области защиты информации.	
ОК 12. Ориентироваться в структуре	- проявление интереса к структуре федеральных органов исполнительной	

федеральных органов исполнительной власти, обеспечивающих информационную безопасность	власти, обеспечивающих информационную безопасность.	