НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Директор НПОУ «ЯКИТ»
_____Л.Н. Цой
«31» августа 2020 г.

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПМ.03
ПРОГРАММНО-АППАРАТНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Специальность: 10.02.01 Организация и технология защиты информации
Квалификация выпускника: Техник по защите информации

Форма обучения: *очная*

Якутск 2020

СОДЕРЖАНИЕ

1.ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Программно-аппаратные и технические средства защиты информации

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО **10.02.01 Организация и технология защиты информации (по отраслям)** в части освоения основного вида профессиональной деятельности (ВПД): **Применение программно-аппаратных и технических средств защиты информации** и соответствующих профессиональных компетенций (ПК):

ПК 3.1.	Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.
ПК 3.2.	Участвовать в эксплуатации систем и средств защиты информации защищаемых объектах.
ПК 3.3.	Проводить регламентные работы и фиксировать отказы средств защиты.
ПК 3.4.	Выявлять и анализировать возможные угрозы информационной безопасности объектов.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в области организации и технологии защиты информации при наличии среднего общего образования. Опыт работы не требуется.

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:

- участия в эксплуатации систем и средств защиты информации защищаемых объектов;
- применения технических средств защиты информации;
- выявления возможных угроз информационной безопасности объектов защиты;

уметь:

- работать с техническими средствами защиты информации;
- работать с защищенными автоматизированными системами;
- передавать информацию по защищенным каналам связи;
- фиксировать отказы в работе средств вычислительной техники;

знать:

- виды, источники и носители защищаемой информации;
- источники опасных сигналов;
- структуру, классификацию и основные характеристики технических каналов утечки информации;
- классификацию технических разведок и методы противодействия им;
- методы и средства технической защиты информации;
- методы скрытия информации;
- программно-аппаратные средства защиты информации;

- структуру подсистемы безопасности операционных систем и выполняемые ею функции;
- средства защиты в вычислительных сетях;
- средства обеспечения защиты информации в системах управления базами данных;
- критерии защищенности компьютерных систем;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.

1.3. Количество часов на освоение рабочей программы профессионального модуля:

максимальной учебной нагрузки обучающегося – **896** часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося –**672** часа, включая:
учебной практики – 144 часа
производственной практики – 108 часов
самостоятельной работы обучающегося – 224 часа;

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися ВПД: **Применение программно-аппаратных и технических средств защиты информации**, в том числе профессиональными и общими компетенциями:

Код	Наименование результата обучения
ПК 3.1.	Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.
ПК 3.2.	Участвовать в эксплуатации систем и средств защиты информации защищаемых объектах.
ПК 3.3.	Проводить регламентные работы и фиксировать отказы средств защиты.
ПК 3.4.	Выявлять и анализировать возможные угрозы информационной безопасности объектов.
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10	Применять математический аппарат для решения профессиональных задач.
ОК 11	Оценивать значимость документов, применяемых в профессиональной деятельности.
ОК 12	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

3.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Код ПК	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
МДК.03.01. Технические методы и средства, технологии защиты информации		**284**	**192**	**82**	**15**	**92**			
ПК 3.1.-3.2.	**Раздел 1. Концепция инженерно-технической защиты информации**	**14**	8	4		6			
ПК 3.1.-3.3.	**Раздел 2. Теоретические основы инженерно-технической защиты информации**	**88**	58	22		30			
ПК 3.1.-3.4.	**Раздел 3. Технические основы добывания и инженерно-технической защиты информации**	**104**	68	40		36			
ПК 3.1.-ПК 3.4.	**Раздел 4. Организационные основы инженерно-технической защиты информации**	**26**	18	10		8			
ПК 3.1.-ПК 3.4.	**Раздел 5. Методическое обеспечение инженерно-технической защиты информации**	**52**	40	6		12			

МДК.03.02. Программно-аппаратные средства защиты информации		**360**	**228**	**98**	**15**	**132**			
ПК 3.3. ПК 3.4.	**Раздел 1. Подсистемы защиты современных операционных систем**	**148**	102	56		46			
ПК 3.1.-3.2. ПК 3.4.	**Раздел 2. Защита информации в вычислительных сетях**	**104**	64	18		40			
ПК 3.1.-ПК 3.4.	**Раздел 3. Защита информации в системах управления базами данных**	**52**	26	16		26			
ПК 3.1.-ПК 3.4.	**Раздел 4. Антивирусная защита компьютерных систем**	**56**	36	8		20			
ПК 3.1.-3.4.	**Учебная практика**	**144**						144	
ПК 3.1.-3.4.	**Производственная практика, (по профилю специальности)**, часов	**108**							108
Всего:		**896**	**420**	**180**	**30**	**224**		**144**	**108**

3.2. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)	Объем часов	Уровень освоения
1	**2**	**3**	**4**
МДК. 03.01. Технические методы и средства, технологии защиты информации		**284**	
Раздел 1. Концепция инженерно-технической защиты информации		**8**	
Тема 1.1. Системный подход к защите информации	**Содержание**	**4**	**1**
	1. Системный подход к инженерно-технической защите информации	2	
	2. Основные положения концепции инженерно-технической защиты информации	2	
	Практические работы	**4**	**2**
	1. Основные положения системного подхода к инженерно-технической защите информации	2	
	2. Принципы построения системы инженерно-технической защиты информации	2	
Раздел 2. Теоретические основы инженерно-технической защиты информации		**58**	
Тема 2.1. Характеристика защищаемой информации	**Содержание**	**4**	**1**
	1. Характеристика защищаемой информации	2	
	2. Демаскирующие признаки объектов защиты	2	
	Практические работы	**4**	**2-3**
	1. Определение количества информации в сообщении, передаваемого по каналам связи	2	
	2. Определение вероятности обнаружения объекта определенной признаковой структуры	2	
Тема 2.2. Характеристика угроз безопасности информации	**Содержание**	**2**	**1**
	1. Характеристика угроз безопасности информации	2	
	Практические работы	**2**	**2**
	1. Анализ угроз информационной безопасности	2	
Тема 2.3. Побочные электромагнитные излучения и наводки	**Содержание**	**2**	**1**
	1. Побочные электромагнитные излучения и наводки	2	
	Практические работы	**2**	**2**
	1. Побочные электромагнитные излучения и наводки средств вычислительной техники	2	
Тема 2.4. Технические каналы утечки информации	**Содержание**	**10**	**1-2**
	1. Технические каналы утечки информации	2	
	2. Акустические каналы утечки информации	2	

	3.	Оптические каналы утечки информации	2	
	4.	Радиоэлектронные каналы утечки информации	2	
	5.	Вещественные каналы утечки информации	2	
	Практические работы		**8**	**3**
	1.	Оценка риска утечки информации по оптическому каналу	2	
	2.	Оценка акустической защищѐнности на основе «метода формантной разборчивости»	4	
	3.	Оценка утечки информации по радиоканалу при использовании специальных технических средств	2	
Тема 2.5.Методы добывания информации	**Содержание**		**2**	**1**
	1.	Методы добывания информации	2	
	Практические работы		**2**	**2**
	1.	Классификация технической разведки	2	
Тема 2.6. Методы инженерно-технической защиты информации	**Содержание**		**14**	**1-2**
	1.	Методы инженерно-технической защиты информации	2	
	2.	Методы физической защиты информации	2	
	3.	Методы противодействия наблюдению	2	
	4.	Методы противодействия подслушиванию	2	
	5.	Обнаружение и подавление закладных устройств	2	
	6.	Методы предотвращения несанкционированной записи речевой информации и подавления опасных сигналов акустоэлектрических преобразователей	2	
	7.	Экранирование побочных излучений и наводок. Методы предотвращения утечки информации по вещественному каналу	2	
	Практические работы		**4**	**2**
	1.	Классификация методов инженерно-технической защиты информации	2	
	2.	Характеристика методов физической защиты информации	2	
	Контрольные работы		**2**	
	1.	Контрольная работа: «Теоретические основы инженерно-технической защиты информации»	2	
Раздел 3. Технические основы добывания и инженерно-технической защиты информации			**68**	
Тема 3.1. Характеристика средств технической разведки	**Содержание**		**10**	**1**
	1.	Характеристика средств технической разведки	2	
	2.	Технические средства подслушивания	2	
	3.	Средства скрытного наблюдения	2	
	4.	Средства перехвата сигналов	2	
	5.	Средства добывания информации о радиоактивных веществах	2	
	Практические работы		**12**	**2-3**
	1.	Классификация технических средств добывания информации	2	
	2.	Технические средства подслушивания и их возможности	2	
	3.	Средства скрытного наблюдения и их возможности	2	
	4.	Средства перехвата сигналов	2	
	5.	Закладные устройства	2	
	6.	Средства добывания информации о радиоактивных веществах	2	

Тема 3.2. Система инженерно-технической защиты информации	**Содержание**		**4**	**1-2**
	1.	Структура системы инженерно-технической защиты информации	2	
	2.	Управление силами и средствами системы инженерно-технической защиты информации	2	
	Практические работы		**4**	**2**
	1.	Аудит комплексной защиты информации предприятия	2	
	2.	Анализ угроз и рисков комплексной защиты информации с использованием систем ГРИФ и КОНДОР	2	
Тема 3.3. Средства инженерной защиты и технической охраны объектов	**Содержание**		**4**	**1**
	1.	Средства инженерной защиты	2	
	2.	Средства технической охраны объектов	2	
	Практические работы		**6**	**2-3**
	1.	Типы извещателей	2	
	2.	Извещатель пожарный дымовой оптико-электронный автономный ИПД-3.4	2	
	3.	Выбор средств видеонаблюдения и мест их установки	2	
Тема 3.4. Средства предотвращения утечки информации	**Содержание**		**10**	**1-2**
	1.	Средства противодействия наблюдению	2	
	2.	Средства звукоизоляции и звукопоглощения акустического сигнала	2	
	3.	Средства предотвращения утечки информации с помощью закладных подслушивающих устройств	2	
	4.	Средства контроля помещений на отсутствие закладных устройств	2	
	5.	Средства предотвращения утечки информации через ПЭМИН	2	
	Практические работы		**18**	**3**
	1.	Средства радиоконтроля. Многофункциональные комплексы «АРК-Д1ТИ» и «НАВИГАТОР-П6-Г»	2	
	2.	Устройства контроля и защиты проводных линий	2	
	3.	Программно-аппаратный комплекс «Спрут-7»	2	
	4.	Сравнительный анализ программно-аппаратных комплексов для проведения акустических и виброакустических измерений	2	
	5.	Нелинейные локаторы. Нелинейный радиолокатор Онега-2М	2	
	6.	Металлодетекторы. Досмотрово-сигнальный комплекс АКА 7202М	2	
	7.	Рентгеновские установки. Портативная рентгенотелевизионная установка «НОРКА».	2	
	8.	Средства подавления радиоэлектронных и звукозаписывающих устройств	2	
	9.	Средства защиты цепей питания и заземления	2	
Раздел 4. Организационные основы инженерно-технической защиты информации			**18**	
Тема 4.1. Организация инженерно-технической защиты информации	**Содержание**		**6**	**2**
	1.	Задачи и структура государственной системы инженерно-технической защиты информации	2	
	2.	Организация инженерно-технической защиты информации на предприятиях (в организациях, учреждениях)	2	
	3.	Нормативно-правовая база инженерно-технической защиты информации	2	
	Практические работы		**6**	**3**
	1.	Современное состояние и тенденции развития технических средств защиты информации российского производства	4	
	2.	Детектор закладных устройств СС-308+	2	

Тема 4.2. Типовые меры по инженерно-технической защите информации	**Содержание**		**2**	**2**
	1.	Типовые меры по инженерно-технической защите информации	2	
	Практические работы		**4**	**3**
	1.	Обнаружение закладных устройств с помощью прибора СС-308+	4	
Раздел 5. Методическое обеспечение инженерно-технической защиты информации			**25**	
Тема 5.1. Рекомендации по моделированию системы инженерно-технической защиты информации	**Содержание**		**19**	**2**
	1.	Моделирование системы ИТЗИ	2	
	2.	Методические рекомендации по моделированию угроз информации	2	
	3.	Оценка угроз оптических и акустических каналов утечки информации	2	
	4.	Оценка угроз радиоэлектронных и вещественных каналов утечки информации	2	
	5.	Методические рекомендации по организации физической защиты источников информации	2	
	6.	Методические рекомендации по предотвращению утечки информации	2	
	7.	Моделирование кабинета руководителя организации как объекта инженерно-технической защиты информации	2	
	8.	Моделирование угроз информации в кабинете руководителя организации	2	
	9.	Нейтрализация угроз информации в кабинете руководителя организации	2	
	Практические работы		**6**	**3**
	1.	Моделирование кабинета лаборатории автоматизированного проектирования технологических процессов и программирования систем с ЧПУ как объекта защиты	2	
	2.	Моделирование угроз информации в кабинете лаборатории автоматизированного проектирования технологических процессов и программирования систем с ЧПУ	2	
	3.	Меры по защите информации в кабинете лаборатории автоматизированного проектирования технологических процессов и программирования систем с ЧПУ	2	
Консультации к курсовому проектированию	**Содержание**		**15**	
	1.	Разработка плана работы	2	
	2.	Подбор литературных источников	2	
	3.	Изучение литературы, выделение нужного материала, работа с конспектом	2	
	4.	Изучение литературы, выделение нужного материала, работа с конспектом	2	
	5.	Сбор и обработка информации	2	
	6.	Сбор и обработка информации	2	
	7.	Подготовка приложений к курсовой работе	2	
	8.	Подготовка приложений к курсовой работе	1	
Самостоятельная работа студента при изучении МДК.03.01.			**92**	

Подготовка доклада на тему «Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей». Подготовка доклада на тему «Технический контроль эффективности мер защиты информации». Подготовка доклада на тему «Элементарный электрический излучатель». Презентация на тему «Каналы утечки информации при передаче по каналам связи». Подготовка доклада на тему «Элементарный магнитный излучатель». Подготовка доклада на тему «Электромагнитные каналы утечки информации ТСПИ». Подготовка доклада на тему «Каналы утечки информации за счет паразитных связей». Презентация на тему «Демаскирующие признаки объектов». Презентация на тему «Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра». Презентация на тему «Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра». Презентация на тему «Демаскирующие признаки радиоэлектронных средств». Презентация на тему «Способы скрытого видеонаблюдения и съемки». Презентация на тему «Каналы утечки информации». Подготовка доклада на тему «Виды зон безопасности». Подготовка презентации по теме " Прослушивание помещений ". Презентация на тему «Сканирующие радиоприемники». Презентация на тему «Индикаторы электромагнитного поля». Подготовка доклада на тему «Методы технического контроля». Презентация на тему «Анализаторы спектра, радиочастомеры». Подготовка доклада на тему «Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М» Подготовка доклада на тему «Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья». Подготовка доклада на тему « Биометрические устройства для обеспечения безопасности». Подготовка доклада на тему «Аттестация объектов, лицензирование деятельности по защите информации». Подготовка доклада на тему «Средства нейтрализации угроз». Подготовка доклада на тему «Скрытие и защита информации от утечки по техническим каналам». Подготовка доклада на тему «Виды контроля эффективности инженерно-технической защиты информации». Подготовка доклада на тему Средства управлений и передачи извещений». Подготовка доклада на тему «Средства маскировки и дезинформации в оптическом и радиодиапазонах». Изучение технических устройств обеспечения защиты информации (сравнительная таблица). Подготовка доклада на тему «Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке». Подготовка доклада на тему «Основные задачи, структура и характеристика государственной системы противодействия технической разведке». Презентация на тему «Средства обнаружения, локализации и подавления сигналов закладных устройств». Презентация на тему «Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления». Презентация на тему «Генераторы линейного и пространственного зашумления». Презентация на тему «Средства управления и передачи извещений. Автоматизированные интегральные системы охраны». Презентация на тему «Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз». Презентация на тему «Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом».		
Дифференцированный зачет	**1**	

МДК.03.02 Программно-аппаратные средства защиты информации			**360**	
Раздел 1. Подсистемы защиты современных операционных систем			**102**	
Тема 1.1. Методы и средства защиты информации от несанкционированного доступа	**Содержание**		**8**	**2**
	1.	Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. Требования к комплексным системам защиты информации (КСЗИ)	2	
	2.	Способы несанкционированного доступа к информации в компьютерных системах и защиты от него	2	
	3.	Идентификация и аутентификация пользователей	2	
	4.	Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях	2	
	Практические работы		**4**	**2**
	1.	Способы несанкционированного доступа и защиты от него компьютерных систем	2	
	2.	Условия надежной программно-аппаратной защиты от локального несанкционированного доступа к информации	2	
Тема 1.2. Подсистемы защиты информации в ОС Windows и UNIX	**Содержание**		**14**	**2**
	1.	Проблемы обеспечения безопасности ОС.	2	
	2.	Архитектура подсистемы защиты ОС	2	
	3.	Разграничение доступа к объектам ОС. Аудит	2	
	4.	Обеспечение безопасности ОС UNIX	2	
	5.	Защита файлов и средства аудита в ОС UNIX	2	
	6.	Особенности организации безопасности в Windows Vista	2	
	7.	Безопасность системы Windows Vista при работе в сети	2	
	Практические работы		**8**	**3**
	1.	Аудит информационных процессов операционной системе Windows	4	
	2.	Аудит реестра в операционной системе Windows	4	
Тема 1.3. Криптографические методы и средства обеспечения информационной безопасности	**Содержание**		**10**	**2**
	1.	Основные понятия криптографической защиты информации	2	
	2.	Симметричные и асимметричные криптосистемы шифрования	2	
	3.	Электронная цифровая подпись и функция хеширования	2	
	4.	Классификация криптографических алгоритмов	2	
	5.	Алгоритм шифрования RSA. Алгоритмы цифровой подписи.	2	
	Практические работы		**18**	**3**
	1.	Парольная защита	2	
	2.	Архивирование с паролем	2	
	3.	Шифр простой замены. Таблица Вижинера	2	
	4.	Криптографические методы преобразования информации. Методы замены и подстановки	4	
	5.	Аналитические методы шифрования	4	
	6.	Исследование электронно-цифровой подписи (ЭЦП) на основе алгоритма RSA	4	

Тема 1.4 Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ	**Содержание**		**10**	**2**
	1.	Программно-аппаратные средства защиты информации.	2	
	2.	Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	2	
	3.	Построение системы защиты на основе комплекса СЗИ НСД «Аккорд-АМД3»	2	
	4.	Электронный замок «СОБОЛЬ», USB-ключ.	2	
	5.	Построение системы защиты на основе комплекса СЗИ «SecretNet 7.0»	2	
	Практические работы		**24**	**3**
	1.	Построение системы защиты на основе комплекса СЗИ НСД «Аккорд-АМД3»	4	
	2.	Электронный замок «Соболь», USB-ключ.	4	
	3.	Комплекс СЗИ «SecretNet 7.0»	4	
	4.	Обеспечение разграничения доступа к защищаемой информации средствами комплекса СЗИ «SecretNet 7.0»	4	
	5.	Построение системы защиты на основе комплекса СЗИ «SecretNet 7.0»	4	
	6.	Интеграция «SecretNet 7.0» и ПАК «Соболь»- преимущества решения и особенности работы	4	
Тема 1.5 Защита программ	**Содержание**		**4**	**2**
	1.	Защита программ от изучения.	2	
	2.	Защита от изменения и контроль целостности.	2	
	Практические работы		**2**	**2**
	1.	Защита программ от изучения, разрушающих программных воздействий, изменения и контроль целостности.	2	
Раздел 2. Защита информации в вычислительных сетях			**64**	
Тема 2.1. Обеспечение межсетевого взаимодействия	**Содержание**		**8**	**2**
	1.	Основы сетевого и межсетевого взаимодействия	2	
	2.	Политика безопасности	2	
	3.	Управление и уменьшение рисков	2	
	4.	Аудит информационной безопасности	2	
	Практические работы		**4**	**3**
	1.	Изучение теоретических аспектов, механизмов работы и вариантов совместного применения межсетевого экрана и сетевого сканера на примере ПО Agnitum Outpost и XSpider	4	
Тема 2.2. Удаленные сетевые атаки	**Содержание**		**10**	**2**
	1.	Понятие атаки. Типы угроз. Классификация атак по основным механизмам реализации угроз	2	
	2.	Атаки «отказ в обслуживании»	2	
	3.	Примеры атак	2	
	4.	Классификации удаленных атак	2	
	5.	Оценивание степени серьезности атак	2	
	Практические работы		**4**	**3**
	1.	Защита от несанкционированного доступа и сетевых хакерских атак	4	
Тема 2.3. Технологии межсетевых экранов	**Содержание**		**8**	**2**
	1.	Развитие технологий межсетевого экранирования	2	
	2.	Особенности функционирования различных межсетевых экранов	2	
	3.	Обход межсетевых экранов	2	
	4.	Требования и показатели защищенности межсетевых экранов	2	

	Практические работы		**4**	**3**
	1.	Защита сетей с применением межсетевых экранов	4	
Тема 2.4. Системы обнаружений атак и вторжений	**Содержание**		**16**	2
	1.	Модели систем обнаружения вторжений	2	
	2.	Классификация систем обнаружения вторжений. Обнаружение сигнатур	2	
	3.	Системы обнаружения вторжений	2	
	4.	Системы обнаружения аномалий	2	
	5.	Другие методы обнаружения вторжений	2	
	6.	Методы обхода систем обнаружения вторжений	2	
	7.	Тестирование систем обнаружения вторжений	2	
	8.	Системы предупреждения вторжений	2	
	Практические работы		**4**	**3**
	1.	Защитник Windows	2	
	2.	Брандмауэр Windows	2	
Тема 2.5 Виртуальные частные сети	**Содержание**		**4**	**2**
	1.	Понятие виртуальной частной сети, еѐ предназначение	2	
	2.	Средства защиты виртуальной частной сети	2	
	Практические работы		**2**	**2**
	1.	Виртуальные частные сети и их предназначение	2	
Раздел 3. Защита информации электронного документооборота и в системах управления базами данных			**26**	
Тема 3.1. Защита информации в системах управления базами данных	**Содержание**		**6**	**2**
	1.	Концепция электронного документооборота	2	
	2.	Защита баз данных	2	
	3.	Средства защиты в СУБД Microsoft Access и Oracle	2	
	Практические работы		**8**	**3**
	1.	Проектирование и нормализация БД	4	
	2.	Защита баз данных Microsoft Access	4	
Тема 3.2. Защита корпоративного почтового документооборота	**Содержание**		**4**	**2**
	1.	Комплексный подход к защите корпоративного почтового документооборота	2	
	2.	Защита системы электронного документооборота DIRECTUM	2	
	Практические работы		**8**	**3**
	1.	Защита документов Microsoft Word	4	
	2.	Защита книг Microsoft Excel	4	
Раздел 4. Антивирусная защита компьютерных систем			**30**	
Тема 4.1. Понятие вредоносной программы	**Содержание**		**13**	**3**
	1.	Типичные предпосылки к внедрению компьютерных вирусов.	2	
	2.	Классификация компьютерных вирусов и вредоносных программ.	2	
	3.	Троянские кони. Сетевые черви. Потайные ходы. Руткиты.	2	
	4.	Вредоносные программы для мобильных устройств	2	

	5.	Проверка систем на вирусы.	2	
	6.	Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения.	2	
	Практические работы		**8**	**3**
	1.	Основные признаки присутствия на компьютере вредоносных программ	4	
	2.	Профилактика заражения вирусами компьютерных систем	4	
Консультации по курсовому проектированию	**Содержание**		**15**	
	1.	Подготовка чернового варианта курсовой работы	2	
	2.	Подготовка чернового варианта курсовой работы	2	
	3.	Корректировка содержания после проверки	2	
	4.	Подготовка чистового варианта, оформление работы.	2	
	5.	Подготовка чистового варианта, оформление работы.	2	
	6.	Сдача работы на проверку и рецензию	2	
	7.	Выполнение рекомендаций руководителя	2	
	8.	Выполнение рекомендаций руководителя	1	
Самостоятельная работа студента при изучении МДК.03.02			**132**	
Презентация на тему «Управление доступом в операционных системах». Подготовка доклада на тему «Построение политики безопасности, обеспечивающей высокую защищенность от программных закладок». Презентация на тему «Идентификация и аутентификация пользователей операционных систем». Подготовка доклада на тему «Аудит в операционных системах». Подготовка доклада на тему «Интеграция защищенных операционных систем в защищенную сеть». Презентация на тему «Подотчетность действий, повторное использование объектов, точность и надежность обслуживания, защита обмена данных». Подготовка доклада на тему «Реализация подсистем безопасности». Презентация на тему «Средства обеспечения безопасности в ОС семейств UNIX и Windows». Подготовка доклада на тему «Структура защищенности ОС». Подготовка доклада на тему «Домены безопасности». Презентация на тему «Критерии защищенности ОС». Подготовка доклада на тему «Структура защищенной ОС». Подготовка доклада на тему «Механизмы защиты ОС». Презентация на тему «Криптографические алгоритмы». Подготовка доклада на тему «Идентификация и установление личности». Презентация на тему «Защита против электронного и электромагнитного перехвата». Презентация на тему «Аутентификация, авторизация, администрирование действий пользователей». Подготовка доклада на тему «Методы аутентификации, использующие пароли и PIN-коды». Подготовка доклада на тему «Строгая аутентификация». Презентация на тему «Биометрическая аутентификация пользователя». Подготовка доклада на тему «Особенности функционирования межсетевых экранов на различных уровнях модели OSI». Презентация на тему «Концепция построений виртуальных защищенных сетей VPN». Подготовка доклада на тему «Достоинства применения технологий VPN». Презентация на тему «Задачи и средства администратора безопасности баз данных». Подготовка доклада на тему «Журнализация. Регистрация действий пользователя». Презентация на тему «Управление набором регистрируемых событий. Анализ регистрационной информации».				
Дифференцированный зачет			**1**	

Учебная практика	**144**	
1-2. Создание защищѐнного канала передачи данных. 3-4. Настройка идентификации пользователей в автоматизированной системе. 5-6. Тестирование пожарно-охранной сигнализации. 7-8. Отслеживание журнала аудита. 9-10. Проверка системы на вирусы и несанкционированный доступ. 11-12. Анализ и оценка каналов утечки информации. 13-14. Исключения несанкционированного доступа к информационным ресурсам. 15-16. Приемы, методы и способы выявления неисправностей в компьютерах, компьютерных системах и сетях. 17. Описание (моделирования) объектов защиты; 18-19. Выявление демаскирующих признаков объектов защиты. 20-21. Использование диагностического оборудования для диагностики технического состояния инженерно-технических средств защиты информации 22-23. Использование программно-аппаратных комплексов. 24. Дифференцированный зачет		
Производственная практика	**108**	
1-3. Проверка защищенности объектов информатизации. 4-7. Осуществление работ с техническими средствами защиты информации. 8-11. Осуществление работ с защищенными автоматизированными системами. 12-13. Передача информации по защищенным каналам связи. 14-15. Выявление возможных угроз информационной безопасности. 16-17. Использование программно-аппаратных комплексов для диагностики технического состояния инженерно-технических средств защиты информации. 18.Дифференцированный зачет		

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие:

кабинета

Информационной безопасности;

лабораторий

Компьютерной техники;

Программно-аппаратных и технических средств защиты информации;

Оборудование учебного кабинета и рабочих мест кабинета **Информационной безопасности**:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект нормативной документации;
- плакаты;
- компьютеры с программным обеспечением;
- мультимедийные средства обучения;
- комплект стендов;
- комплект лабораторно-практических работ

Оборудование лаборатории и рабочих мест лаборатории: **Компьютерной техники;**

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

Лаборатория: **Программно-аппаратных и технических средств защиты информации:**

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

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Мельников В.П., Клеймѐнов С.А., Петраков А.М. Информационная безопасность: Учебное пособие для СПО. – М.: Академия, 2018
2. Платонов В.В. Программно-аппаратные средства защиты информации: Учебное пособие для СПО. – М.: Академия, 2017.

Дополнительные источники:

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие. – СПб: НИУ ИТМО, 2018.
2. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. – СПб: Академия, 2018.
3. Хорев П.Б. методы и средства защиты информации в компьютерных системах. М.: Академия, 2018.
4. Девянин П.Н. Программно-аппаратные средства защиты от несанкционированного доступа к компьютерным криптографическим системам обработки информации. М.: РИО МИЭМ, 2018.
5. Серегин В.В., Сидоров В.А. Атака через интернет. СПб.: НПО «МИР», 2019.
6. Спесивцев А.В. Защита информации в персональных ЭВМ. М.: Радио и связь, 2019.
7. Корчма М.Ю. Обзор программно-аппаратных комплексов для оценки защищенности речевой информации от утечки по акустоэлектрическому каналу. – Сборник научных трудов НГТУ, 2017, № 3(81), с. 134-145.

Рекомендуемые источники:

1. Торокин А. А. Инженерно-техническая защита информации: Учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности. – М.: Гелиос АРВ, 2017.
2. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В.Технические средства и методы защиты информации: Учебник для вузов. – М.: Машиностроение, 2019.
3. Проскурин В.Г. Защита программ и данных. М.: Академия», 2018.
4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. М.: ИНФРА-М, 2017.
5. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: ИНФРА-М, 2017.

Интернет-ресурсы:

1. Единое окно доступа к образовательным ресурсам. Форма доступа: http://window.edu.ru.
2. Единая коллекция цифровых образовательных ресурсов. Форма доступа: http://school-collection.edu.ru.
3. http://wwwcom.ru/

4.3. Общие требования к организации образовательного процесса

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

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

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

дисциплины:

ОП.04 Технические средства информатизации

ОП.05 Базы данных

ОП.06 Основы информационной безопасности

Профессиональный модуль содержит два междисциплинарных курса МДК.03.01. Технические методы и средства, технологии защиты информации, МДК.03.02. Программно-аппаратные средства защиты информации, в которых предусмотрено изучение теоретического материала, а также выполнение практических работ, которые проводятся в лабораториях техникума под руководством преподавателя. Для выполнения практических работ разрабатываются инструкционные карты. После каждого раздела предусмотрена внеаудиторная самостоятельная работа, направленная на расширение кругозора по изучаемой тематике.

По междисциплинарным курсам профессионального модуля, учебной и производственной практик предусмотрена аттестация в форме дифференцированного зачета. Дифференцированный зачет может быть проведен в устной форме, выполнен в форме реферата или решения ситуационных задач, подтверждающих профессиональную компетентность обучающихся.

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

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

Оценка качества подготовки обучающихся осуществляется в двух направлениях:

- Оценка уровня освоения дисциплины;
- Оценка компетенций обучающихся.

По профессиональному модулю рабочей программой предусмотрена учебная и производственная практики.

Задачей производственной практики является:

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

- развитие общих и профессиональных компетенций;

Производственная практика проводится после освоения материала профессионального модуля. Обязательным условием допуска к производственной практике (по профилю специальности) в рамках профессионального модуля **Применение программно-аппаратных и технических средств защиты информации** является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля**.**

По профессиональному модулю обучающимися выполняется курсовая работа (проект).

При работе над курсовыми работами (проектами) обучающимся оказываются консультации.

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

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

Экзамен (квалификационный) проводится по окончании освоения рабочей программы профессионального модуля и представляет собой форму независимой оценки результатов обучения с участием работодателей. Условием допуска к экзамену (квалификационному) является успешное освоение обучающимися всех элементов программы профессионального модуля – МДК, учебной и производственной практики.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): наличие высшего профессионального образования, соответствующего профилю модуля **Программно-аппаратные и технические средства защиты информации** и специальности **10.02.01 Организация и технология защиты информации.**

Педагогические кадры, обеспечивающие обучение по данному профессиональному модулю должны иметь высшее образование, соответствующее профилю профессионального модуля, и проходить повышение квалификации и (или) стажировку в профильных организациях не реже одного раза в три года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой

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

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК.3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.	- обоснованность выбора технических и программно-аппаратных средств защиты информации; - грамотное применение	Экспертная оценка выполненной работы. Текущий контроль в форме: - защиты практических работ;

	технических и программно-аппаратных средств защиты информации; - правильность освоения возможностей работоспособности компонентов систем защиты информации.	- контрольных работ по темам МДК. - наблюдение за выполнением практических работ. Дифференцированные зачеты по производственной практике и по каждому из разделов профессионального модуля. Дифференцированные зачеты по МДК. Защита курсового проекта. Комплексный экзамен по профессиональному модулю.
ПК.3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектах.	-умение решать частные технические задачи, возникающие при эксплуатации систем и средств защиты информации; - умение осуществлять мероприятия по выявлению и оценке свойств каналов утечки информации.	
ПК.3.3. Проводить регламентные работы и фиксировать отказы средств защиты.	- точность и скорость диагностики нарушений эксплуатационных характеристик средств защиты; -качество анализа эксплуатационных свойств средств защиты; - проверка технического состояния средств защиты; - умения проводить техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность средств защиты.	
ПК.3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.	- умение выявлять и анализировать возможные угрозы информационной безопасности объектов.	

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Принимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности	демонстрация интереса к будущей профессии;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	выбор и применение методов и способов решения; профессиональных задач в области защиты информации предприятий; оценка эффективности и качества выполнения;	
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	решение стандартных и нестандартных профессиональных задач в области защиты информации;	
Осуществлять поиск и использование информации, необходимые для эффективного выполнения профессиональных задач, профессионального и личностного развития	эффективный поиск необходимой информации, использование различных источников, включая электронные;	
Использовать информационно-коммуникационные технологии в профессиональной деятельности	работа с прикладными программами в области защиты информации;	
Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями	взаимодействие с обучающимися и преподавателями в ходе обучения;	
Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	самоанализ и коррекция результатов собственной работы;	
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение	организация самостоятельных занятий при изучении профессионального модуля;	

квалификации		
Ориентироваться в условиях частой смены технологий профессиональной деятельности	анализ инноваций в области защиты информации	
Применять математический аппарат для решения профессиональных задач	применение математического анализа для решения профессиональных задач	
Оценивать значимость документов, применяемых в профессиональной деятельности	самостоятельная оценка значимости документов, применяемых в профессиональной деятельности	
Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность	анализ структуры федеральных органов исполнительной власти, обеспечивающих информационную безопасность	