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

Рабочая программа профессионального модуля ПМ03 Применение программно-аппаратных и технических средств защиты информации

специальность 10.02.01 Организация и технология защиты информации

Нижний Новгород

2021 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности (специальностям) среднего профессионального образования (далее СПО) 10.02.01 Организация и технология защиты информации, входящей в укрупненную группу 10.00.00 Информационная безопасность

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

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля является частью примерной основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.01 «Организация и технология защиты информации» в части освоения основного вида профессиональной деятельности (ВПД**):** Программно-аппаратные и технические средства 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 объектов.

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.

ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

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

владеть:
- профессиональной терминологией:
- навыками внедрения и эксплуатации современных средств программно-аппаратной защиты информации;
- способами выявления и нейтрализации программ разрушающего действия;
- навыками разработки и использования межсетевых экранов и систем обнаружения и предотвращения вторжений.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:
максимальной учебной нагрузки обучающегося – 654 часа, включая:
обязательной аудиторной учебной нагрузки обучающегося – 436 часов;
самостоятельной работы обучающегося – 218 часов;
учебной практики – 252 часов;
производственной практики – 144 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности Программно-аппаратные и технические средства защиты информации, в том числе профессиональными (ПК) и общими (ОК) 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 объектов
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

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

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 *если предусмотрена рассредоточенная практика)*
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 3.1-3.4	**МДК 03.01. Технология применения технических методов и средств защиты информации**	**366**	**244**	**124**		**122**			
ПК 3.1-3.4	**МДК 03.02. Технология использования программно-аппаратных средств защиты информации**	**288**	**192**	**86**	**30**	**96**			
	В том числе:								
ПК 3.1-3.4	**Учебная практика**							**252**	
ПК 3.1-3.4	**Производственная практика** (по профилю специальности)								**144**
	Всего:	**654**	**436**	**210**	**30**	**218**		**252**	

* 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. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов МДК	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)		Объем часов	ЛР, ОК, ПК
1	**2**		**3**	**4**
ПМ 03. Применение программно-аппаратных и технических средств защиты информации				ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
МДК 03.01 Технические методы и средства, технологии защиты информации			**366**	ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
			4	
Введение	1	Виды информации, защищаемой техническими средствами.	**2**	
	2	Свойства информации, влияющие на возможности ее защиты	**2**	
Раздел 1. Концепция инженерно-технической защиты информации				ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
Тема 1.1. Системный подход к защите информации	**Содержание**		**4**	
	3	Системный подход к инженерно-технической защите информации	**2**	
	4	Основные положения концепции инженерно-технической защиты информации	**2**	

Раздел 2. Теоретические основы инженерно-технической защиты информации				ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
Тема 2.1. Характеристика защищаемой информации	**Содержание**		**4**	
	5	Характеристика защищаемой информации	**2**	
	6	Демаскирующие признаки объектов защиты	**2**	
	Практические занятия		**2**	
	1	Классификация угроз	**2**	
Тема 2.2. Характеристика угроз безопасности информации	**Содержание**		**2**	
	7	Характеристика угроз безопасности информации	**2**	
	Практические занятия		**2**	
	2	Классификация объектов защиты	**2**	
Тема 2.3. Побочные электромагнитные излучения и наводки	**Содержание**		**2**	
	8	Побочные электромагнитные излучения и наводки	**2**	
Тема 2.4. Технические каналы утечки информации	**Содержание**		**2**	
	9	Технические каналы утечки информации	**2**	
	Практические занятия		**4**	
	3	Классификация технических каналов утечки информации. Информационный сигнал	**4**	

		и его характеристики		
	Содержание		**2**	
	10	Акустические каналы утечки информации	**2**	
	Практические занятия		**4**	
	4	Средства акустической разведки	**4**	
	Содержание		**6**	
	11	Вещественные каналы утечки информации	**2**	
	12	Оптические каналы утечки информации	**2**	
	13	Радиоэлектронные каналы утечки информации	**2**	
	Практические занятия		**4**	
	5	Средства радио- и радиотехнической разведки	**4**	
Тема 2.5.Методы добывания информации	**Содержание**		**4**	
	14	Методы добывания информации	**2**	
	15	Методы инженерно-технической защиты информации	**2**	
	Практические занятия		**4**	
	6	Системы защиты территории и помещений	**4**	
	Содержание		**2**	

16	Методы физической защиты информации	**2**	
Практические занятия		**8**	
7	Системы охранной, тревожной и пожарной сигнализации	**4**	
8	Системы контроля и управления доступом	**4**	
Содержание		**4**	
17	Методы противодействия наблюдению	**2**	
18	Методы противодействия подслушиванию	**2**	
Практические занятия		**4**	
9	Защита акустической (речевой) информации	**4**	
Содержание		**10**	
19	Обнаружение и подавление закладных устройств	**2**	
20	Методы предотвращения несанкционированной записи речевой информации	**2**	
21	Методы подавления опасных сигналов акустоэлектрических преобразователей	**2**	
22	Экранирование побочных излучений и наводок	**2**	
23	Методы предотвращения утечки информации по вещественным каналам	**2**	
Практические занятия		**4**	

	10	Телевизионные системы безопасности	**4**	
Раздел 3. Технические основы добывания и инженерно-технической защиты информации				
Тема 3.1. Характеристика средств технической разведки.	**Содержание**		**12**	ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
	24	Характеристика средств технической разведки	**2**	
	25	Технические средства подслушивания	**2**	
	26	Средства скрытного наблюдения	**2**	
	27	Средства перехвата сигналов	**2**	
	28	Средства добывания информации о радиоактивных веществах	**2**	
	29	Средства добывания информации о химических веществах	**2**	
Тема 3.2. Система инженерно-технической защиты информации	**Содержание**		**4**	
	30	Структура системы инженерно-технической защиты информации	**2**	
	31	Управление силами и средствами системы инженерно-технической защиты информации	**2**	
	Практические занятия		**12**	
	11	Характеристика объекта защиты	**6**	

	12	Формирование требований к физической защите объекта	**6**	
Тема 3.3. Средства инженерной защиты и технической охраны объектов	**Содержание**		**4**	
	32	Средства инженерной защиты	**2**	
	33	Средства технической охраны объектов	**2**	
	Практические занятия		**18**	
	13	Монтаж датчиков пожарной и охранной сигнализации	**6**	
	14	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	**6**	
	15	Рассмотрение принципов устройства, работы и применения средств контроля доступа	**6**	
Тема 3.4. Средства предотвращения утечки информации		**Содержание**	**2**	
	34	Средства противодействия наблюдению	**2**	
	Практические занятия		**6**	
	16	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения	**6**	
	Содержание		**8**	
	35	Средства звукоизоляции и звукопоглощения акустического сигнала	**2**	
	36	Средства предотвращения утечки информации с помощью закладных подслушивающих устройств	**2**	

	37	Средства контроля помещений на отсутствие закладных устройств	**2**	
	38	Средства предотвращения утечки информации через ПЭМИН	**2**	
		Практические занятия	**18**	
	17	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации	**6**	
	18	Выбор и обоснование средств подсистемы задержки	**6**	
	19	Разработка структурной схемы и спецификации оборудования	**6**	
Раздел 4. Организационные основы инженерно-технической защиты информации				
		Содержание	**2**	ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
Тема 4.1. **Организация инженерно-технической защиты информации**	39	Задачи и структура государственной системы инженерно-технической защитыинформации	**2**	
	Содержание		**4**	
	40	Организация инженерно-технической защиты информации на предприятиях (ворганизациях, учреждениях)	**4**	
	Практические занятия		**2**	
	20	Задачи и функции органов по технической защите информации в РФ	**2**	

	Содержание		**2**	
	41	Нормативно-правовая база инженерно-технической защиты информации	**2**	
		Практические занятия	**14**	
	21	Законодательная и нормативная база правового регулирования вопросов технической защиты информации	**4**	
	22	Лицензирование деятельности в области защиты информации	**4**	
	23	Изучение общего порядка аттестации объекта информатизации по требованиям безопасности информации	**6**	
Тема 4.2. **Типовые меры по инженерно-технической защите информации**		**Содержание**	**2**	
	42	Типовые меры по инженерно-технической защите информации	**2**	
		Практические занятия	**6**	
	24	Эксплуатация инженерно-технических средств физической защиты	**6**	
Раздел 5. Методическое обеспечение инженерно-технической защиты информации				
Тема 5.1. **Рекомендации по моделированию системы инженерно-технической защиты информации**		**Содержание**	**34**	ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
	43	Моделирование системы ИТЗИ	**2**	

	44	Методические рекомендации по моделированию угроз информации	**4**	
	45	Оценка угроз оптических и акустических каналов утечки информации	**4**	
	46	Оценка угроз радиоэлектронных и вещественных каналов утечки информации	**4**	
	47	Методические рекомендации по организации физической защиты источников информации	**4**	
	48	Методические рекомендации по предотвращению утечки информации	**4**	
	49	Моделирование кабинета руководителя организации как объекта инженерно-технической защиты информации	**4**	
	50	Моделирование угроз информации в кабинете руководителя организации	**4**	
	51	Нейтрализация угроз информации в кабинете руководителя организации	**4**	
		Практические занятия	**12**	
	25	Моделирование технической разведки по исходным данным для объекта информатизации	**6**	
	26	Моделирование инженерно-технической системы защиты информации по исходным данным для объекта информатизации	**6**	
	52	Дифференцированный зачет	**2**	
Итого			**244**	
Самостоятельная работа обучающихся: Подготовка доклада на тему «Классификация и характеристика охранных, охранно-пожарных и пожарных			**122**	

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».			
МДК 03.02 Программно-аппаратные средства защиты информации		**288**	ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
Раздел 1. Подсистемы защиты современных операционных систем			ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
Тема 1.1. Методы и средства защиты информации от несанкционированного доступа	**Содержание**	**8**	
	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 занятия	**2**	

	1.	Идентификация и аутентификация пользователей операционных систем	**2**	
Тема 1.2. Подсистемы защиты информации в ОС Windows и UNIX	**Содержание**		**4**	
	5	Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС Разграничение доступа к объектам ОС. Аудит	**2**	
	6	Особенности организации безопасности в Windows 10 .Безопасность системы Windows 10 при работе в сети	**2**	
	Практические занятия		**8**	
	2	Реализация подсистемы защиты операционной системы Windows	**4**	
	3	Управление доступом в операционных системах	**4**	
	Содержание		**2**	
	7	Обеспечение безопасности ОС UNIX. Защита файлов и средства аудита в ОС UNIX		
	Практические занятия		**48**	
	4	Установка операционной системы Linux. Основные принципы функционирования ОС Linux	**4**	
	5	Терминал и командная оболочка операционной системы Linux	**4**	
	6	Изучение файловой системы и функций по обработке и управлению данными	**4**	
	7	Процессы в операционной системе Linux	**4**	
	8	Организация ввода-вывода в ОС Linux	**4**	
	9	Создание и выполнение командных файлов в пользовательской среде ОС Linux	**4**	
	10	Удаленный доступ в Linux	**4**	
	11	Управление пользователями и обеспечение безопасности в ОС Linux	**4**	
	12	Администрирование DNS-сервера в ОС Linux	**4**	
	13	Маршрутизация в ОС Linux. Межсетевое экранирование в Linux	**4**	
	14	Обеспечение доступа в сеть Интернет ОС Linux.	**4**	
	15	Разработка подсистемы защиты операционной системы Linux	**4**	
Тема 1.3. Криптографические методы и средства обеспечения информационной	**Содержание**		**6**	
	8	Основные понятия криптографической защиты информации. Симметричные и асимметричные криптосистемы шифрования	**2**	
	9	Электронная цифровая подпись и функция хеширования	**2**	
	10	Классификация криптографических алгоритмов. Алгоритм шифрования RSA.	**2**	

безопасности		Алгоритмы цифровой подписи.		
	Практические занятия		**8**	
	16	Электронная цифровая подпись.	**4**	
	17	Программно-аппаратное шифрование данных при их хранении.	**4**	
Тема 1.4 Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ	**Содержание**		**6**	
	11	Программно-аппаратные средства защиты информации.	**2**	
	12	Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	**2**	
	13	СЗИ НСД «Аккорд-АМД3» Электронный замок СОБОЛЬ», USB-ключ. СЗИ «SecretNet 7.0»	**2**	
Тема 1.5 Защита программ	**Содержание**		**2**	
	14	Защита программ от изучения. Защита от изменения и контроль целостности	**2**	
Раздел 2. Защита информации в вычислительных сетях				ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
Тема 2.1. Обеспечение межсетевого взаимодействия	**Содержание**		**6**	
	15	Основы сетевого и межсетевого взаимодействия	**2**	
	16	Политика безопасности. Аудит информационной безопасности	**2**	
	17	Управление и уменьшение рисков	**2**	
Тема 2.2. Удаленные сетевые атаки	**Содержание**		**6**	
	18	Понятие атаки. Типы угроз. Классификация атак по основным механизмам реализации угроз	**2**	
	19	Атаки «отказ в обслуживании». Классификации и примеры удаленных атак	**2**	
	20	Оценка степени серьезности атак	**2**	
Тема 2.3. Технологии межсетевых экранов	**Содержание**		**4**	
	21	Развитие технологий межсетевого экранирования, особенности их функционирования, требования и показатели защищенности	**2**	
	22	Обход межсетевых экранов	**2**	
	Практические занятия		**4**	

	18	Межсетевые экраны.	**4**	
Тема 2.4. Системы обнаружений атак и вторжений	**Содержание**		**10**	
	23	Модели систем обнаружения вторжений	**2**	
	24	Классификация систем обнаружения вторжений. Обнаружение сигнатур	**2**	
	25	Системы обнаружения вторжений. Системы обнаружения аномалий.	**2**	
	26	Методы обхода систем обнаружения вторжений	**2**	
	27	Системы предупреждения вторжений	**2**	
	Практические занятия		**8**	
	19	Программное восстановление данных.	**4**	
	20	Обнаружение и предотвращение вторжений.	**4**	
Тема 2.5 Виртуальные частные сети	**Содержание**		**4**	
	28	Понятие виртуальной частной сети, предназначение	**2**	
	29	Средства защиты виртуальной частной сети	**2**	
Раздел 3. Защита информации электронного документооборота и в системах управления базами данных				ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
Тема 3.1. Защита информации в системах управлениябазами данных	**Содержание**		**4**	
	30	Концепция электронного документооборота	**2**	
	31	Средства защиты в СУБД Microsoft Access и Oracle	**2**	
	Практические занятия		**4**	
	21	Организация защиты данных СУБД	**4**	
Тема 3.2. Защита	**Содержание**		**4**	

корпоративного почтового ящика	32	Комплексный подход к защите корпоративного почтового документооборота	**2**	
	33	Защита системы электронного документооборота DIRECTUM	**2**	
Раздел 4. Антивирусная защита компьютерных систем				ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
Тема 4.1. Понятие вредоносной программы	**Содержание**		**8**	
	34	Типичные предпосылки к внедрению компьютерных вирусов.	**2**	
	35	Троянские кони. Сетевые черви. Потайные ходы. Руткиты.	**2**	
	36	Вредоносные программы для мобильных устройств	**2**	
	37	Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения.	**2**	
	Практические занятия		**4**	
	22	Организация защиты данных на ПК от компьютерных вирусов	**4**	
	38	Дифференцированный зачет	**2**	
Курсовое проектирование			**30**	ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4
Итого			**192**	
Самостоятельная работа обучающихся: Самостоятельная работа обучающихся: 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			**96**	

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». 101 3 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».		
Учебная практика Анализ и оценка каналов утечки информации. Монтаж различных типов датчиков. Определение каналов утечки ПЭМИН. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	**252**	ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4

Тестирование пожарно-охранной сигнализации. Применение промышленных осциллографов, частотомеров и генераторов, и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. Настройка идентификации пользователей в автоматизированной системе. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления. Реализация защиты от утечки по цепям электропитания Выявление демаскирующих признаков объектов защиты. Описание (моделирование) объектов защиты; Разработка организационных и технических мероприятий по заданию преподавателя; Установка и настройка технических средств защиты информации. Проверка системы на вирусы и несанкционированный доступ. Исключения несанкционированного доступа к информационным ресурсам. Приемы, методы и способы выявления неисправностей в компьютерах, компьютерных системах и сетях. Создание защищённого канала передачи данных. Проведение аттестации объектов информатизации. Промежуточная аттестация в форме дифференцированного зачета		
Производственная практика Вводный инструктаж. Изучение источников и носителей защищаемой информации предприятия. Выявление потенциальных угроз информационной безопасности предприятия, технических каналов утечки информации. Изучение инженерной защиты и технической охраны объектов информации, имеющихся на предприятии. Изучение имеющихся технических средств информатизации и программного обеспечения предприятия. Предмет и задачи программно-аппаратной защиты информации. Изучение информационного обеспечение предприятия. Методы и средства ограничения доступа к компонентам ЭВМ.	**144**	ЛР13-15, ОК 1 - 12 ПК 3.1 - 3.4

Защита программного обеспечения предприятия от потенциального несанкционированного копирования. Изучения методов хранения ключевой информации на предприятии. Изучение обеспечения работоспособности программного обеспечения АИС предприятия. Формирование отчетной документации по результатам работ. Дифференцированный зачёт		

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Материально-техническое обеспечение

Реализация программы модуля предполагает наличие:
учебного кабинета

- Информационной безопасности;
- Систем и сетей передачи

информации.лаборатории

- Программно-аппаратных и технических средств защиты информации иэлектронного документооборота;

Оборудование учебного кабинета и рабочих мест:
кабинет Информационной безопасности:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект нормативной документации;
- компьютеры с программным обеспечением;
- мультимедийные средства

обучения. кабинет Систем и сетей
передачи информации.

- посадочные места по количеству студентов;
- рабочее место преподавателя;
- рабочие места студентов;
- комплект учебно-наглядных пособий;
- комплект учебно-методической документации;
- комплект презентаций к уроку;
- комплект раздаточного

материала.Технические средства
обучения:

- компьютер с необходимым программным обеспечением и мультимедиапроектор сэкраном.

Оборудование рабочих мест обучающихся:

- монитор;
- системный блок;
- клавиатура.

Оборудование места преподавателя:

- компьютер;
- принтер;
- сканер;
- колонки.

Оборудование лаборатории и рабочих мест:
Программно-аппаратных и технических средств защиты информации и

электронного документооборота;

- посадочные места, рассчитанные на подгруппу;
- рабочее место преподавателя;
- компьютеры с лицензионным программным обеспечением;
- специализированное программное обеспечение.

4.2. Информационное обеспечение обучения

Основные источники:

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMAR.
2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.
3. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин ; под редакцией Т. С. Кулаковой. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.

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.

Интернет-ресурсы:

1. Единое окно доступа к образовательным ресурсам. Форма доступа: http://window.edu.ru.
2. Единая коллекция цифровых образовательных ресурсов. Форма доступа: http://schoolcollection. edu.ru.
3. http://www.mascom.ru/
4. http://nelk.ru/
5. http://www.laborkomplekt.ru/
6. http://pro-spec.ru/

7. http://www.bnti.ru
8. http://www.inside-zi.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:

ПМ.02 Организация и технология работы с конфиденциальными документами.

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.

По междисциплинарным курсам профессионального модуля предусмотрена промежуточная аттестация в форме дифференцированного зачета.

Результатом учебной и производственной практики является дифференцированный зачет.

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

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

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу и профессиональному модулю: высшее профессиональное образование, соответствующее профилю преподаваемого междисциплинарного курса и профессионального модуля. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального цикла с обязательной стажировкой в профильных организациях не реже 1-го раза в 3 года.

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.3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.	- обоснованность выбора технических и программно-аппаратных средств защиты информации; - грамотное применение технических и программно-аппаратных средств защиты информации; - правильность освоения возможностей работоспособности компонентов систем защиты информации.	Экспертная оценка выполненной работы. Текущий контроль в форме: - защиты практических работ; - наблюдение за выполнением практических работ. Дифференцированные зачеты по учебной производственной практик, и по каждому из разделов профессионального модуля. Дифференцированный зачетпо 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.	

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

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.	- демонстрация понимания целей и задач профессиональной деятельности; - осознание способов деятельности, выбор средств, адекватных ее целям и задачам	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методови способов решения профессиональных задач в организации и технологии защиты информации; - оценка эффективности и качества выполнения работ.	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- рациональность решения стандартных профессиональных задач в области защиты информации; - аргументированность самоанализа выполнения профессиональных задач	
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	- эффективный поиск необходимой информации; - использование различных источников, включая электронные;	

ОК 5. Использовать информационно-коммуникационные технологиив профессиональной деятельности.	- использование программ автоматизации профессиональной деятельности (владеть навыками работы в специальных программах, а также текстовых и табличных редакторах, программах по	

	созданию презентаций).	
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	- взаимодействие с обучающимися, преподавателями, мастерами, руководителями практик от предприятия в ходе обучения	
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных),результат выполнения заданий.	- самоанализ и коррекция результатов собственной работы при выполнении практических заданий в группе, при подготовке к внеклассным мероприятиям	
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	- организация самостоятельных занятий при изучении профессиональногомодуля	
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	- анализ инноваций в области защиты информации	
ОК 10. Применять математический аппарат для решения профессиональных задач.	- применение математического анализа для решения профессиональных задач	
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.	- самостоятельная оценка значимости документов, применяемых в профессиональной деятельности	
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	- анализ структуры федеральных органов исполнительной власти, обеспечивающих информационную безопасность	