Негосударственное частное учреждение
Профессиональная образовательная организация
«Уральский институт подготовки кадров «21-й век»

УТВЕРЖДАЮ:
Председатель учебно-методического совета
заместитель директора
_____ М.В. Федорук
«09» августа 2018 г.

Программа профессионального модуля
ПМ.03. Программно-аппаратные и технические средства защиты информации
по специальности
10.02.01 Организация и технология защиты информации

Нижний Тагил
2018 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования

10.02.01 Организация и технология защиты информации

Организация-разработчик НЧУ ПОО «Уральский институт подготовки кадров «21-й век»

Составитель: преподаватель, к.п.н., доцент Райхерт Т.Н.

Программа рассмотрена и утверждена на заседании кафедры Информационных технологий

«3» августа 2018 г. протокол № 1

Зав. кафедрой ИТ _____ А.А. Трепалин

СОДЕРЖАНИЕ

стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Применение программно-аппаратных и технических средства защиты информации

1.1. Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 090905 Организация и технология защиты информации, входящей в укрупненную группу специальностей 090000 Информационная безопасность, в части освоения основного вида профессиональной деятельности Применение программно-аппаратных и технических средства защиты информации 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.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке работников в области защиты информации при наличии среднего (полного) общего образования. Опыт работы не требуется.

1.2. Цели и задачи профессионального 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 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 документов.

1.3. Количество часов, отведенных на освоение программы профессионального модуля:

всего - 576, в том числе:

максимальной учебной нагрузки обучающегося - 324 часа, включая:

обязательной аудиторной учебной нагрузки обучающегося - 90 часа;

самостоятельной работы обучающегося - 234 часов;

учебной практики по профилю специальности - 144 часа

производственной практики по профилю специальности - 108 часов.

Формой аттестации по профессиональному модулю являются:

МДК.03.01 Технические методы и средства, технологии защиты информации: зачет – 2,3 семестр;

МДК.03.02 Программно-аппаратные средства защиты информации: зачет – 2 семестр, экзамен – 4 семестр.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности Применение программно-аппаратных и технических средства защиты информации, в том числе профессиональными 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.
ПК3.3.	Проводить регламентные работы и фиксировать отказы средств защиты.
ПК 3.4.	Выявлять и анализировать возможные угрозы информационной безопасности объектов.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Объем профессионального модуля и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	***324***
Обязательная аудиторная учебная нагрузка (всего)	***90***
в том числе:	
лабораторные занятия	***40***
практические занятия	
контрольные работы	
курсовая работа (проект) *(если предусмотрено)*	***30***
Самостоятельная работа обучающегося (всего)	***234***
в том числе:	
внеаудиторная самостоятельная работа	
самостоятельная работа над курсовой работой (проектом) *(если предусмотрено)*	
Указываются другие виды самостоятельной работы при их наличии (расчетно-графическая работа, домашняя работа и т.п.).	
Промежуточная аттестация в 6 семестре в форме дифференцированного зачета *Промежуточная аттестация* в 7 семестре в форме экзамена	

2.1. Тематический план профессионального модуля
ПМ.03 Программно-аппаратные и технические средства защиты информации

Код ПК	Наименования разделов ПМ	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 работыи практические занятия, часов	курсовая работа (проект), часов	Всего, часов	курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
МДК.03.01. Технические методы и средства, технологии защиты информации		108	20	10	-	88			
МДК.03.02. Программно-аппаратные средства защиты информации		216	70	30	30-	146			
УП.03 Учебная практика								144	
ПП.03 Производственная практика									108
	Всего:	324	90	40	30-	234	-	144	108

средств защиты информации

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работ (проект)		Объем часов	Уро-ень осво ния
1	2		3	4
МДК.03.01.Технические методы и средства, технологии защиты информации			20	
РАЗДЕЛ 1. Концепция инженерно-технической защиты информации				
Тема 1.1. Системный подход к защите информации	Содержание			
	1.	Основные концептуальные положения инженерно-технической защиты информации. Структура и основные характеристики технических каналов утечки информации.	1	2
	2.	Характеристика инженерно-технической защиты информации как области информационной безопасности.		
	3.	Основные проблемы инженерно-технической защиты информации.		
	4.	Представление сил и средств защиты информации в виде системы.		
	5.	Основные параметры системы защиты информации. Классификация технических каналов утечки информации.		
	Практические занятия			
	1.	Определение разрешения объектов защиты от возможного наблюдения с использованием современных визуально-оптических и оптико-электронных приборов	0,5	
	2.	Расчёт уровней речевых сигналов в местах возможного нахождения злоумышленника или его подслушивающих технических средств	0,5	
	3.	Оценка утечки информации по радиоканалу при использовании специальных технических средств (закладных устройств) и за счёт побочных электромагнитных излучений	1	

РАЗДЕЛ 2. Теоретические основы инженерно-технической защиты информации				
Тема 2.1. Информация как предмет защиты. Источники опасных сигналов	Содержание			
	1.	Особенности информации как предмета защиты	1	2
	2.	Свойства информации. Виды, источники и носители защищаемой информации.		
	3.	Демаскирующие признаки объектов наблюдения, сигналов и веществ.		
	4.	Понятие о текущей и эталонной признаковой структуре.		
	5.	Состав и краткая характеристика основных и вспомогательных технических средств и систем. Источники опасных сигналов.		
	Практические занятия			
	1.	Расчёт зон 1 и 2 для основных технических средств и систем, размещённых в помещении	1	
РАЗДЕЛ 3. Технические средства добывания и инженерно-технической защиты информации				
Тема 3.1 Средства технической разведки		Содержание		
	1.	Классификация технических разведок и методы противодействия им. Визуально-оптические приборы. Фотоаппараты. Оптоэлектрические приборы наблюдения в видимом и инфракрасном диапазонах	1	2
	2.	Акустические приемники. Направленные микрофоны.		
	3.	Структура комплексов перехвата.		
	4.	Особенности сканирующих радиоприемников.		
	5.	Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки		
	Практические занятия			
	1.	Работа с техническими средствами защиты информации. Технические средства защиты речевой информации в телефонных линиях	0,5	

	2.	Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, излучающих в радио- и инфракрасном диапазонах	0,5	
Тема 3.2 Средства инженерной защиты и технической охраны	Содержание		1	2
	1.	Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации		
	2.	Средства управления доступом.		
	3.	Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей.		
	4.	Средства видеоконтроля и видеоохраны		2
	5.	Автоматизированные интегральные системы охраны.		
	Практические занятия			
	1.	Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, использующих силовые линии сети переменного тока и линии систем пожарной и охранной сигнализаций	0,5	
	2.	Контроль эффективности защиты речевой информации	0,5	
Раздел 4. Организационные основы инженерно-технической защиты информации				
Тема 4.1. Государственная система защиты информации. Контроль эффективности инженерно-технической защиты информации.		Содержание	1	2
	1.	Основные задачи, структура и характеристика государственной системы противодействия технической разведке.		
	2.	Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.		
	3.	Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности.		

	4.	Термины и определения в области технической защиты информации: объект информатизации		
	5.	Место технической защиты информации в государственной системе защиты информации в Российской Федерации.		
	6.	Цели и задачи защиты информации от утечки информации по техническим каналам	0,5	
	7.	Нормативные документы по технической защите информации.		
	8.	Технические методы и средства защиты информации		
Раздел 5. Технические каналы утечки информации				
Тема 5.1. Основные показатели технических средств	Содержание			
	1.	Оценка дальности перехвата сигналов.	0,5	
	2.	Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.		
	Практические занятия			
	1.	Микрофонный эффект в основных и вспомогательных технических средствах.	0,5	
	2.	Устройства несанкционированного съема акустической информации.	0,5	
Тема 5.2. Технические каналы утечки информации, обрабатываемой СВТ и АС	Содержание			2
	1.	Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	0,5	
	2.	Работа с защищенными автоматизированными системами. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ.		

	Практические занятия			
	1.	Методы и средства съема информации с телефонных линий.	0,5	
	2.	Побочные электромагнитные излучения средств вычислительной техники.	0,5	
Тема 5.3 Технические каналы утечки акустической (речевой) информации.	Содержание			2
	1.	Общая характеристика и классификация технических каналов утечки акустической информации. Передача информации по защищенным	0,5	
	2.	Прямые акустические каналы утечки речевой информации.		
	3.	Средства акустической разведки и их технические характеристики.		
	Практические занятия			
	1.	Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях.	1	
	2.	Выявление информативных частот ПЭМИН ПК.	1	
	3.	Выделение речевого сигнала на фоне шумов и помех.	1	
Раздел 6. Способы и средства защиты информации от утечки по техническим каналам				
Тема 6.1. Способы и средства защиты информации, обрабатываемой	Содержание			2
	1.	Методы и средства технической защиты информации, объектов информатизации и их классификация.	1	

средствами вычислительной автоматизированными системами	2.	Требования к системам электропитания и заземления основных технических средств и систем.		
	4.	Помехоподавляющие фильтры.		
	5.	Защищённые средства вычислительной техники.		
Тема 6.2.Способы и средства защиты выделенных помещений от утечки речевой информации каналам	Содержание			
	1.	Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.	1	2
	2.	Звукоизоляция выделенных помещений. Звукопоглощающие материалы.		
	3.	Системы и средства виброакустической маскировки.		
	4.	Способы и средства защиты вспомогательных технических средств и систем.		
	5.	Специальные технические средства подавления электронных устройств перехвата речевой информации		
Раздел 7. Методы и средства контроля эффективности технической защиты информации				
Тема 7.1. Методы и средства контроля	Содержание			
	1.	Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Фиксация отказов в работе средств вычислительной техники.	1	2
	2.	Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений; порядок проведения измерений.		
	3.	Методика оценки возможностей средств технической разведки по перехвату побочных электромагнитных излучений и наводок средств вычислительной техники.		

4.	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам.		
5.	Принципы построения и использования охранных, охранно-пожарных и пожарных извещателей. План-схема защиты помещений средствами охранных, охранно-пожарных и пожарных извещателей.		2
6.	Принципы моделирования объектов защиты. Технический канал утечки информации, создаваемый СВТ. Характеристики речевого сигнала. Основные характеристики систем радиолокационного наблюдения Экранированные помещения		

Самостоятельная работа обучающегося 1. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. 2. Элементарный электрический излучатель 3. Элементарный магнитный излучатель 4. Электромагнитные каналы утечки информации ТСПИ 5. Технические каналы утечки информации при передаче ее по каналам связи 6. Каналы утечки информации за счет паразитных связей. 7. Демаскирующие признаки объектов 8. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра 9. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра 10. Демаскирующие признаки радиоэлектронных средств 11. Способы скрытого видеонаблюдения и съемки. 12.Индикаторы электромагнитного поля 13. Сканирующие радиоприемники 14. Анализаторы спектра, радиочастотомеры. 15.Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М» 16.Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья». 17. Скрытие и защита информации от утечки по техническим каналам 18. Технический контроль эффективности мер защиты информации. 19. Виды контроля эффективности инженерно-технической защиты информации. 20. Виды зон безопасности. 21. Методы технического контроля. 22. Особенности инструментального контроля эффективности инженерно-технической защиты информации. 23. Аттестация объектов, лицензирование деятельности по защите информации 24. Основные организационные и технические меры по защите информации.	88	

25. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. 26. Основные задачи, структура и характеристика государственной системы противодействия технической разведке. 27. Средства маскировки и дезинформации в оптическом и радиодиапазонах 28. Средства обнаружения, локализации и подавления сигналов закладных устройств 29. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. 30. Генераторы линейного и пространственного зашумления. 31. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны. 32. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. 33. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. 34. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом.		

МДК.03.02.Программно-аппаратные средства защиты информации			70	
Раздел 1. Подсистема защиты современных операционных систем				
Тема 1.1 Подсистема защиты информации в ОС UNIX	Содержание		2	2
	1.	Основные компоненты подсистемы защиты Unix.		
	2.	Файловая система - как основа подсистемы защиты.	1	
	3.	Права доступа к элементам файловой систем. Управление процессами.	1	
	4.	Создание и удаление бюджетов пользователей.	1	
	5.	Основные проблемы с безопасностью и возможные решения в Unix-подобных системах.	1	
	Практические занятия			
	1.	Разработка подсистемы защиты операционной системы Linux	2	
	2.	Реализация подсистемы защиты операционной системы Windows	1	
	3.	Обеспечение защиты вычислительной сети	1	
Тема 1.2. Подсистемы защиты информации в ОС Windows NT	Содержание			2
	1.	Основные компоненты подсистемы защиты Windows NT и Windows 2000	2	

	2.	Политики. Понятие домена.	1	
	3.	Особенности установления доверительных отношений. Создание и удаление бюджетов пользователей.	1	
	Практические занятия			
	1.	Настройка межсетевых экранов для организационной защиты ВС	1	
Тема 1.3 Защита информации при интеграции UNIX и Windows NT.	Содержание		1	2
	1.	Основы взаимодействия элементов гетерогенных сетей. Шлюзы NFS, SMB в Unix. Использование сервера Samba для разделения доступа к сетевым ресурсам в домене Windows NT.		
	Практические занятия			
	1.	Организация защиты данных СУБД SQL Server 2010	1	
	2.	Настройка антивирусной защиты операционной системы Windows	1	
Тема 1.4 Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ	Содержание		2	2
	1.	Программно-аппаратные средства защиты информации. Методы и средства ограничения доступа к компонентам ЭВМ.		
	2.	Структура подсистемы безопасности операционных систем и выполняемые ею функции. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	1	
	3.	Методы и средства хранения ключевой информации.	1	
	Практические занятия			
	1.	Работа с антивирусной программой «Касперский»	1	
	2.	Управление доступом в операционных системах	1	
Тема 1.5. Защита программ	Содержание		2	2
	1.	Защита программ от изучения. Защита от разрушающих программных воздействий. Защита от изменения и контроль целостности.		
	Практические занятия			
	1.	Идентификация и аутентификация пользователей операционных систем.	2	
	2.	Аудит в операционных системах	2	

Раздел 2. Защита информации в вычислительных сетях				
Тема 2.1 Атаки на сетевые службы	Содержание		1	2
	1.	Понятие атаки. Типы угроз. Классификация атак по основным механизмам реализации угроз. Сетевые сканеры.		
	2.	Понятие адаптивности безопасности и системы обнаружение атак.	1	
	Практические занятия			
	1.	Интеграция защищенных операционных систем в защищенную сеть	2	
Тема 2.2. Адаптивная безопасность в ВС	Содержание		2	2
	1.	Понятие адаптивности безопасности и системы обнаружения атак		
	Практические занятия			
	1.	Сетевые атаки	2	
Тема 2.3 Межсетевые экраны	Содержание		2	3
	1.	Понятие межсетевых экранов. Их классификация.		
	Практические снятия			
	1.	Пакетные фильтры и межсетевые экраны	2	
Тема 2.4 Виртуальные сети	Содержание			2
	1.	Понятие виртуальной частной сети, ее предназначение. Средства защиты в вычислительных сетях.	2	
	Практические занятия			
	1.	Средства и методы обеспечения целостности данных в СУБД	2	
Тема 2.5 Политика безопасности	Содержание			2
	1.	Понятие политики информационной безопасности для организации. Основные требования к политике безопасности. Этапы ее разработки.	2	
	Практические занятия			
	1.	Средства и методы обеспечения конфиденциальности данных СУБД	2	
Раздел 3. Защита информации в системах управления базами данных				

Тема 3.1 Понятия безопасности БД	Содержание			2
	1.	Угрозы безопасности БД: общие и специфичные. Требования безопасности БД.	2	
	Практические занятия			
	1.	Особенности защиты распределенных СУБД	2	
Тема 3.2 Критерии защищенности БД	Содержание			2
	1.	Критерии защищенности компьютерных систем. Критерии оценки надежных компьютерных систем. Понятие политики безопасности. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.	2	
	Практические занятия			
	1.	Построение политики безопасности, обеспечивающей высокую защищенность от программных закладок	2	
Тема 3.3 Модели безопасности в СУБД	Содержание			2
	1.	Классификация моделей. Аспекты исследования моделей безопасности.	2	
	Практические занятия			
	1.	Настройка и использование специализированного антивирусного программного обеспечения.	2	
Тема 3.4 Механизмы обеспечения целостности СУБД	Содержание			2
	1.	Средства обеспечения защиты информации в системах управления базами данных. Основные виды и причины возникновения угроз целостности. Способы противодействия.	2	
Раздел 4. Антивирусная защита компьютерных систем				
Тема 4.1	Содержание			

Понятие компьютерного вируса	1.	Типичные предпосылки к внедрению компьютерных вирусов.	2	
	2.	Классификация компьютерных вирусов и вредоносных программ	2	
	3	Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения.	2	2

Самостоятельная работа обучающегося 1. Построение политики безопасности, обеспечивающей высокую защищенность от программных закладок. 2. Управление доступом в операционных системах 3. Идентификация и аутентификация пользователей операционных систем 4. Аудит в операционных системах. 5. Интеграция защищенных операционных систем в защищенную сеть. 6. Подотчетность действий, повторное использование объектов, точность и надежность обслуживания, защита обмена данных. 7. Реализация подсистем безопасности. 8. Средства обеспечения безопасности в ОС семейств UNIX и Windows 9. Структура защищенной ОС 10. Домены безопасности 11. Критерии защищенности ОС 12. Структура защищенной ОС 13. Контрольная работа на тему: «Программно-аппаратные средства защиты информации» 14. Механизмы защиты ОС. 15. Криптографические алгоритмы. Экранирование. Идентификация и установление личности. 16. Защита против электронного и электромагнитного перехвата. Аутентификация, авторизация и администрирование действий пользователей. 17. Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIII-коды. 18. Строгая аутентификация. Биометрическая аутентификация пользователя. 19. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. 20. Концепция построения виртуальных защищенных сетей VPN. 21. VPN-решения для построения защищенных сетей. Достоинства применения технологий VPN. 22. Задачи и средства администратора безопасности баз данных. 23. Журнализация. Регистрация действий пользователя. 24. Управление набором регистрируемых событий. Анализ регистрационной информации.	146	

Курсовая работа Темы курсовых работ 1. Аудит в операционных системах. 2. Интеграция защищенных операционных систем в защищенную сеть. 3. Реализация подсистем безопасности 4. Криптографические алгоритмы. 5. Идентификация и установление личности. 6. Защита против электронного и электромагнитного перехвата. 7. Биометрическая аутентификация пользователя. 8. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. 9. VPN-решения для построения защищенных сетей. 10. Безопасность баз данных. 11. Технические каналы утечки информации при передаче ее по каналам связи 12. Способы скрытого видеонаблюдения и съемки 13. Скрытие и защита информации от утечки по техническим каналам 14. Технический контроль эффективности мер защиты информации 15. Аттестация объектов, лицензирование деятельности по защите информации	30	
Учебная практика (по профилю специальности) Виды работ 1) использовать диагностическое оборудование для диагностики технического состояния инженерно-технических средств защиты информации в условиях учебной лаборатории 2) использовать программно-аппаратные комплексы для диагностики технического состояния инженерно-технических средств защиты информации в условиях учебной лаборатории 3) устанавливать соответствующее ПО для обеспечения работоспособности инженерно-технических средств обеспечения защиты информации в условиях учебной лаборатории	144	

Производственная практика (по профилю специальности) Виды работ 1) использовать диагностическое оборудование для диагностики технического состояния инженерно-технических средств защиты информации в условиях конкретного предприятия 2) использовать программно-аппаратные комплексы для диагностики технического состояния инженерно-технических средств защиты информации в условиях конкретного предприятия 3) устанавливать соответствующее ПО для обеспечения работоспособности инженерно-технических средств обеспечения защиты информации в условиях конкретного предприятия	108	
Всего	486	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1.- ознакомительный (узнавание ранее изученных объектов, свойств)

2.- репродуктивный (выполнение деятельности по образцу, инструкции и под руководством)

3. -продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Материально-техническое обеспечение

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

Оборудование учебного кабинета и рабочих мест кабинета:

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

Технические средства обучения:

- мультимедийный проектор;
- интерактивная доска;
- компьютеры.

4.2. ИНФОРМАЦИАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Вычислительные системы, сети и телекоммуникации: учебное пособие. / А.П. Пятибратов, -М.: Издательство «КноРус», 2013.-376 с.: ил.
2. Шаньгин П.П. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: Издательство «Форум», 2013.-416 с. Рекомендовано МО РФ.

Дополнительные источники:

3. Организация безопасной работы информационных систем: учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др.; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с.: ил. Утверждено УС.
http://biblioclub.ru/index.php?page=book&id=277794
4. Некраха, А.В. Организация конфиденциального делопроизводства и защита информации: учебное пособие / А.В. Некраха, Г.А. Шевцова; Институт информационных наук и технологий безопасности, Российский государственный гуманитарный университет. - М.: Академический проект, 2012. - 222 с.

Рекомендовано УМО. http://biblioclub.ru/index.php?page=book&id=143604
5. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов. - М.: Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. http://biblioclub.ru/index.php?page=book&id=362895
6. Нестеров, С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб: Издательство Политехнического университета, 2014. - 322 с.: схем, табл., ил. http://biblioclub.ru/index.php?page=book&id=363040
7. Организация безопасной работы информационных систем: учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др.; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с.: ил. Утверждено УС. http://biblioclub.ru/index.php?page=book&id=277794
8. Пятибратов, А.П. Вычислительные системы, сети и телекоммуникации: учебник / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко. - 4-е изд., перераб. и доп. - М.: Финансы и статистика, 2013. - 736 с. Рекомендовано МО РФ http://biblioclub.ru/index.php?page=book&id=220195

Интернет-ресурсы:

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

4.3. Общие требования к организации образовательного процесса

Реализация профессионального модуля может проходить независимо от других предметов.

Обязательным условием допуска студентов к производственной практике (по профилю специальности) является завершение теоретического обучения в рамках профессионального модуля ПМ.03 «Применение программно-аппаратных и технических средств защиты информации».

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.	- определение показателей технического состояния программно- аппаратных средства защиты информации; - определение основных положений технического обслуживания и текущего ремонта компонентов подсистем защиты информации; - освоение возможностей восстановления работоспособности компонентов систем защиты информации.	Текущий контроль: - опрос - выполнение практических работ; -защита реферата.
ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.	- выбор программно-аппаратных средств обеспечения защиты информации и их эксплуатация -освоение основных этапов конфигурирования программно- аппаратных средств защиты информации; - освоение методов установки и настройки параметров современных технических средств защиты информации; - освоение основных положений производства, монтажа и эксплуатации программно- аппаратных средств защиты информации	

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.	-выбор методов определения отказов в работе средств защиты информации;	
	- проверка работоспособности и необходимости применения программно-аппаратных средств обеспечения информационной безопасности	Текущий контроль: - опрос - выполнение практических работ; -защита реферата.
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.	- выявление угроз информационной безопасности объектов; - анализ угроз информационной безопасности объектов	