АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01

Эксплуатация автоматизированных информационных систем в защищенном исполнении

2017

Организация-разработчик: АНО ПО «Балтийский информационный техникум»

Разработчики:

Балаклиевский Валерий Давидович, зам. Директора АНО ПО «БИТ»

Япарова Юлия Алексеевна, преподаватель АНО ПО «БИТ»

Рассмотрена на заседании цикловой методической комиссии «информационной безопаснрости» 27 февраля 2017г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля **«Эксплуатация автоматизированных информационных систем»** является частью примерной основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид профессиональной деятельности ***Эксплуатация автоматизированных (информационных) систем в защищенном исполнении*** и соответствующие ему профессиональные компетенции:

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 1	**Эксплуатация автоматизированных (информационных) систем в защищенном исполнении**
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

Содержание профессионального модуля состоит из набора разделов, каждый из которых соответствует конкретной профессиональной компетенции или нескольким компетенциям и направлен на развитие набора универсальных компетенций.

Дескрипторы сформированности компетенций по разделам профессионального модуля.

Спецификация ПК/ разделов профессионального модуля

Формируемые компетенции	***Название раздела***		
	Действия (дескрипторы)	***Умения***	***Знания***
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатацион-	– Решение практических задач установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем;	- осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем	– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных системах и сетях;

ной документации.			
1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	– Решение практических задач администрирования автоматизированных систем в защищенном исполнении;	- организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; - производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации – порядок установки и настройки средств защиты информации в компьютерных системах и сетях;
ПК 1.3 Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	– Решение практических задач по эксплуатации компонентов систем защиты информации автоматизированных систем и обеспечению их бесперебойной работы;	- обеспечивать работоспособность, обнаруживать и устранять неисправности подсистем безопасности автоматизированных систем согласно технической документации	- порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях - принципы основных методов организации бесперебойной работы вычислительной техники и других технических средств информатизации.
ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и	Решение практических задач диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособ-	– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным	- принципы основных методов организации и проведения технического обслуживания вычислительной техники и

восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	ности автоматизированных (информационных) систем в защищенном исполнении	правилам;	других технических средств информатизации.

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных компетенций	Наименование разделов профессионального модуля	Всего часов	Объём времени 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., курсовой проект часов	Всего, часов	в т.ч., курсовой проект, часов		
ПК 1.1-1.4 ОК.1-4, ОК. 9	**МДК 01.01 Эксплуатация подсистем безопасности автоматизированных систем**	**122**	**80**	42		**42**		**34**	**34**
ПК 1.1-.1.4 ОК.1-4, ОК. 9	**МДК 01.02 Эксплуатация компьютерных сетей**	**200**	**140**	72		**60**		**34**	**34**
УП	**Учебная практика**	**72**							
ПП	**Производственная практика**	**72**							
	Всего:	**466**	**364**	**114**		**102**		**72**	**72**

2.2 Тематический план профессионального модуля (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовой проект		Объем часов
1	2		3
МДК 01.01 Эксплуатация подсистем безопасности автоматизированных систем			**122**
Тема 1.1 Автоматизированные системы как объекты обеспечения безопасности информации	**Содержание**		**6**
	1	**Предмет безопасности информации АС** Объекты информационной безопасности АС. Потенциальные угрозы в АС	
	2	**Методы обеспечения безопасности информации в АС** Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа в системе. Разделение привилегий на доступ. Идентификация и установление подлинности объекта (субъекта). Криптографическое преобразование информации в автоматизированных системах	
	3	**Защита информации от утечки** Защита информации от утечки за счет побочного электромагнитного излучения и наводок (ПЭМИН). Методы и средства защиты информации от случайных воздействий. Обеспечения безопасности информации при аварийных ситуациях. Проведение организационных мероприятий по обеспечению безопасности информации в АС	
Тема 1.2 Структура системы обеспечения безопасности информации в АС	**Содержание**		**4**
	1	**Структура системы обеспечения безопасности информации в АС** Основные компоненты и их функции. Регламентация действий пользователей и обслуживающего персонала АС. Система организационно-распорядительных документов по организации защиты информации	
Тема 1.3 Подсистема обеспечения безопасности информации от несанкционированного доступа (НСД)	**Содержание**		**6**
	1	**Подсистема защиты от НСД** Структура подсистемы обеспечения безопасности информации от НСД. Задачи и общие принципы построения подсистемы. Характеристика классов защищенности. Требования к подсистемам СЗИ от НСД в АС. Основные различия и особенности требований в зависимости от конфиденциальной информации. Практическая реализация подсистем СЗИ от НСД	
	Практические занятия		**4**
	Построение матрицы угроз от НСД и матрицы каналов и средств противодействия НСД		

	Разработка матрицы угроз информационного объекта		
	Разработка плана основных этапов по проектированию системы обеспечения безопасности		
	Разработка шаблонов маршрута согласования		
	Разработка шаблона внутренних нормативных документов		
	Разработка примерного плана организации работ по эксплуатации средств безопасности автоматизированных систем		
Тема 1.4 Подсистема обеспечения безопасности от преднамеренного несанкционированного доступа (ПНСД)	**Содержание**		**4**
	1	**Подсистема защиты от ПНСД** Подсистема обеспечения безопасности информации и программного обеспечения от преднамеренного несанкционированного доступа (ПНСД) при вводе, выводе и транспортировке	
	Практические занятия		**8**
	Планирование, создание и изменение учетных записей пользователей		
	Создание и администрирование групп пользователей		
	Изменение параметров учетных записей пользователей		
	Настройка политики учетных записей		
	Настройка параметров безопасности ОС		
	Создание правил согласования		
	Проектирование безопасного управления сетью. Защита EMS.		
Тема 1.5 Подсистема управления средствами обеспечения безопасности от несанкционированного доступа в АС	**Содержание**		**4**
	1	**Подсистема защиты от НСД** Назначение, решаемые задачи и принципы построения подсистемы управления. Состав и назначение средств управления безопасностью информации. Средства регистрации доступа к информации в АС. Информационное обеспечение системы безопасности информации. Организационные меры по контролю и управлению безопасностью информации и АС	
	Практические занятия		**6**
	Анализ политики безопасности АС		
	Анализ политики безопасности в соответствии с бизнес-процессами предприятия		
	Разработка концептуального плана защиты		
	Изучение консоли MMC		
	Учетные записи пользователей, групп		
Тема 1.6 Экономическое обеспечение защиты информации в АС	**Содержание**		**10**
	1	**Правовые аспекты взаимодействия субъектов на рынке информации** Государственная, коммерческая, персональная и профессиональная тайна. Основные	

		принципы и методы защиты информации	
	2	**Основные документы при эксплуатации АС** Основные документы, регламентирующие действия персонала и сотрудников при эксплуатации АС	
	3	**Добывание информации** Органы добывания информации. Источники добывания коммерческой информации	
	4	**Экономическая эффективность защиты информации** Основные методики определения затрат на информационную безопасность. Определение размера целесообразных затрат на обеспечение информационной безопасности. Модель определения зон защиты предприятия в условиях ограниченности средств. Модель распределения работы службы безопасности предприятия	
	Практические занятия		**16**
	Расчет экономической эффективности объектов АС		
	Расчет экономической эффективности проектных решений		
	Составление технического задания на создание автоматизированных систем		
	Классификация объектов АС		
	Выявление каналов утечки в АС		
	Разработка политики безопасности АС		
	Расчет экономической эффективности модернизации локальной сети		
	Расчет экономической эффективности внедрения ПО в образовательном учреждении		
	Расчет экономической эффективности внедрения программного средств на предприятии		
	Оценка экономической эффективности замены оборудования сервера		
	Расчет экономической эффективности комплексной защиты предприятия		
	Расчет экономической эффективности комплексной защиты финансовых учреждений		
	Расчет экономической эффективности комплексной защиты на производстве		
Тема 1.7 Обеспечение безопасности персональных данных	**Содержание**		**4**
	1	**Организационно-правовые основы обеспечения безопасности ПД при их обработке в ИСПД** Основы информационной безопасности. Персональные данные. Законодательство в области защиты персональных данных. Что означает термин «персональные данные». Классификация информационной системы персональных данных. Положения, регламентирующие порядок обработки и защиты персональных данных. Федеральные законы «Об информации, информационных технологиях и о защите информации», «О персональных данных». Указы Президента Российской Федерации, постановления Правительства Российской Федерации, нормативные и методические документы ФСТЭК России, регламен-	

		тирующие деятельность в области обеспечения безопасности ПД при их обработке в ИСПД	
	2	**Выявление угроз безопасности ПД при их обработке в ИСПД и их уязвимых звеньев** Автоматизированная обработка персональных данных. Организационно-распорядительная документация по защите ПД. Классификация угроз безопасности ПД. Угрозы утечки информации по техническим каналам. Угрозы утечки акустической (речевой) информации. Угрозы утечки видовой информации. Угрозы утечки информации по каналам побочных электромагнитных излучений. Угрозы несанкционированного доступа к информации в ИСПД. Характеристика источников угроз несанкционированного доступа в ИСПД. Характеристика уязвимостей ИСПД. Характеристика уязвимостей системного программного обеспечения. Характеристика уязвимостей прикладного программного обеспечения. Характеристика угроз непосредственного доступа в операционную среду ИСПД. Характеристика угроз безопасности ПД, реализуемых с использованием протоколов межсетевого взаимодействия. Характеристика угроз программно-математических воздействий. Характеристика нетрадиционных информационных каналов. Характеристика результатов несанкционированного или случайного доступа.	
	Практические занятия		**6**
	Порядок организации защиты персональных данных		
	Определение уровня защищенности персональных данных		
	Определение требований в соответствии с уровнем защищенности		
	Общее описание угроз безопасности персональных данных		
	Определение актуальности угроз безопасности персональных данных		
	Используемые средства защиты информации в ИСПДн		
Самостоятельная работа при изучении раздела 1 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. Самостоятельное изучение нормативных и разрешительных документов, алгоритмов защиты информации, правил и требований при разработке мероприятий обеспечения безопасности, выполнение организационной и технологической документации по ЕСКД и ЕСТП. Работа над курсовым проектом. **Примерная тематика внеаудиторной самостоятельной работы:** 1 Разработка концепции защиты информационного объекта 2 Разработка модели защиты информационого объекта 3 Анализ журнала аудита ОС на рабочем месте			**42**

4 Построение сводной матрицы угроз информационного объекта 5 Разработка политики безопасности информационного объекта 6 Разработка плана ввода и мероприятий автоматизированной системы 7 Изучение аналитических обзоров в области построения систем безопасности 8 Анализ программного обеспечения в области проектирования и обеспечения безопасности информации 9 Разработка матрицы угроз информационного объекта 10 Анализ журнала аудита ОС на рабочем месте 11 Изучение аналитических обзоров в области построения систем безопасности 12 Анализ аналитических исследований в области распространения вредоносных программ 13 Анализ программного обеспечения в области обеспечения безопасности информации		
Учебная практика **Виды работ:** - разработка плана основных этапов и их содержания по проектированию системы обеспечения безопасности автоматизированной системы - разработка шаблона концепции безопасности организации - разработка шаблона и примерного плана аудита безопасности автоматизированной системы - разработка шаблона сводной матрицы угроз - разработка примерного плана ввода подсистем и средств безопасности автоматизированной системы - разработка шаблонов и регламента оформления технической и технологической документации - разработка экономической части составляющей проекта - разработка частной модели угроз безопасности персональных данных		**36**
Производственная практика (по профилю специальности) **Виды работ:** - участие в ведении основных этапов проектирования системы обеспечения безопасности автоматизированной системы - установление маршрута согласований основных внутренних документов по эксплуатации автоматизированной системы - планирование и проектирование внутренних нормативных документов по введению средств защиты информации в эксплуатацию - участие в организации работ по эксплуатации подсистем и средств безопасности автоматизированной системы - ознакомление с особенностями функционирования систем обеспечения безопасности организации - оформление технической и технологической документации		**36**
МДК 01.02 Эксплуатация компьютерных сетей		**200**
Тема 2.1 Сетевые службы ОС	**Содержание**	**2**
	1 **Сетевые службы ОС** Сетевые файловые системы и вопросы их реализаций. Служба каталогов. Межсетевое взаимодействие	
	Практические занятия	**2**

	Мониторинг, оптимизация и аудит ОС		
Тема 2.2 Сетевая безопасность	**Содержание**		**6**
	1	**Сетевая безопасность Сетевая безопасность** Основные понятия сетевой безопасности. Базовые технологии сетевой безопасности. Технологии аутентификации. Разработка плана защиты	
	Лабораторные работы		**10**
	Настройка политик безопасности ОС		
	Конфигурирование средств безопасности операционных систем		
	Настройка журнала аудита		
	Настройка служб безопасности		
	Управление ресурсами операционной системы		
	Практические занятия		**10**
	Модель ISO/OSI и задачи обеспечения безопасности в открытых системах		
	Восстановление сетевой операционной системы		
	Администрирование сетевой ОС		
	Аудит, отвечающих за безопасность разделов реестра ОС		
Тема 2.3 Локальные сети и их топологии	**Содержание**		**6**
	1	**Локальные сети и топологии** Место и роль локальных сетей при обеспечении безопасности автоматизированных систем. Локальные сети как объект защиты информации. Топология локальных сетей сравнительная характеристика	
	2	**Система безопасности в сетях** Принципы построения системы безопасности информации в сетях. Потенциальные угрозы и задачи безопасности информации в локальных сетях	
Тема 2.4 Среды передачи данных	**Содержание**		**6**
	1	**Среды передачи данных** Среда передачи данных на витой паре и кабельных системах. Бескабельные каналы связи. Согласование, экранирование и гальваническая развязка линий связи. Механизмы безопасности информации в трактах передачи данных и в каналах связи. Рекомендации по безопасности информации в телекоммуникационных каналах связи	
Тема 2.5 Пакеты, протоколы и методы управления обменом	**Содержание**		**6**
	1	**Сетевые пакеты, протоколы** Назначение и адресация пакетов. Структура пакетов. Методы управления обменом. Сравнение особенностей топологий. Сравнительная характеристика протоколов TCP/IP и IPv6. Протокол IPsec	

Тема 2.6 Уровни сетевой архитектуры	**Содержание**		**6**
	1	**Уровни сетевой архитектуры** Эталонная модель открытых систем ISO/OSI. Уровни взаимодействия открытых систем. Аппаратные ресурсы локальных сетей. Стандартные протоколы и стандартные программные средства	
Тема 2.7 Стандартные локальные сети и подключение к глобальным сетям	**Содержание**		**6**
	1	**Стандарты сетей** Сравнительная характеристика их технологий и безопасности. Особенности подключения к глобальным сетям. Согласование стандартов, технологий, методов	
	Практические занятия		**8**
	IP адресация		
	Классы сетей		
	Формирование подсетей. Маска подсети		
	Расчет маски при разных условиях		
Тема 2.8 Защита информации в локальных сетях	**Содержание**		**6**
	1	**Защита информации в сетях** Система безопасности информации в трактах передачи данных автоматизированной системы. Основные задачи и принципы построения. Средства управления защитой информации в локальных сетях	
	2	**Криптографические методы защиты** Классические алгоритмы шифрования данных при передаче в сетях. Стандартные методы шифрования в сети. Программные средства защиты информации	
	3	**Межсетевые экраны** Межсетевые экраны – технология сетевой защиты. Функции межсетевых экранов. Особенности функционирования и схемы защиты на базе межсетевых экранов. Виртуальные защищенные сети – технология сетевой защиты	
	Лабораторные работы		**8**
	Настройка межсетевого экрана в ОС Windows XP		
	Настройка режима фильтрации		
	Настройка межсетевого экрана в ОС Linux		
	Практические занятия		**10**
	Организация защищенного канала передачи данных		
	Организация виртуального частного канала передачи данных VPN		
	Организация Wi-Fi связи		
	Технологии беспроводной передачи данных		

Тема 2.9 Сетевые алгоритмы. Стандартные сегменты сети	**Содержание**		**6**
	1	**Сетевые алгоритмы** Управление доступом к информации в сети передачи в АС. Методы управления обменом. Система защиты информации от несанкционированного доступа в локальных сетях	
	2	**Алгоритм доступа к сети** Оценка производительности сети. Использование помехоустойчивых кодов для обнаружения ошибок в сети. Характеристики помехоустойчивых кодов. Циклические коды	
	3	**Стандартны сегменты сети** Сравнительные характеристики безопасности сегментов	
Тема 2.10 Конфигурирование сети. Проектирование сети и расчет	**Содержание**		**6**
	1	**Конфигурирование сети** Выбор конфигурации сетей. Правила модели. Проектирование сети. Выбор размера сети и ее структуры. Выбор оборудования. Выбор сетевых программных средств	
	2	**Обнаружение сетевых атак** Оценка уровня безопасности информации от преднамеренного несанкционированного доступа в локальных сетях. Технологии обнаружения сетевых атак и технологии противодействия	
	Лабораторные работы		**10**
	Оценка уровня безопасности информации в сетях		
	Конфигурирование сетевых средств безопасности		
	Настройка сетевых политик безопасности		
	Настройка сетевых служб безопасности		
	Практические занятия		**4**
	Настройка сетевой информационной среды в условиях повышенного риска вторжения		
	Аудит сетевых ресурсов и служб		
Тема 2.11 Удаленные и распределенные хранилища данных	**Содержание**		**6**
	Удаленные и распределенные хранилища данных Удаленные базы данных, режим доступа. Дата-центры. Организация распределенных баз данных.		
	Практические занятия		**12**
	1	Настройка сетевого доступа к базе данных.	
	2	Конфигурирование сетевого доступа к базам данных	
	3	Настройка политик безопасности удаленного доступа	
	4	Настройка служб безопасности	
	5	Настройка служб безопасности удаленного доступа	

Тема 2.12 Защита данных при передаче в сети	**Содержание**	**6**
	Защита данных при передаче в сети Режимы шифрования при передаче данных в сети. Основные технологии, применяемые в сетевых операционных системах.	
Самостоятельная работа при изучении раздела 2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. Самостоятельное изучение программных средств шифрования, их возможности и ограничения защиты данных, изучение правил и требований при работе с сетевыми информационными ресурсами, выполнение технологической документации по ЕСКД и ЕСТП. **Примерная тематика внеаудиторной самостоятельной работы:** 1 Настройка политик сетевой безопасности 2 Настройка журнала аудита и анализ записей работы сетевых служб 3 Контроль и управление сетевыми службами 4 Управление сетевыми ресурсами 5 Тестирование внешнего ПО для администрирования и мониторинга параметров сети 6 Разработка сетевых приложений-служб 7 Настройка программных средств шифрования и политик безопасности при передаче данных в сети 8 Установка и настройка работы процедур шифрования внешних средств 9 Контроль и управление процедурами и службами шифрования информации 10 Разработка сетевых приложений-служб управления шифрованием информации		**60**
Учебная практика **Виды работ:** - конфигурирование сетевых средств безопасности - проведение мероприятий по предотвращению конфликтов сетевых устройств и ресурсов - настройка сетевых политик безопасности - настройка сетевых служб безопасности - аудит сетевых ресурсов и служб - программирование сценариев и служб для управления сетевыми ресурсами - конфигурирование средств шифрования для безопасной передаче в сети - настройка политик безопасности обеспечивающих шифрование сетевого трафика - настройка служб безопасности обеспечивающих реализацию и контроль за процедурой шифрования сетевого трафика - программирование сценариев и служб для шифрования данных		**36**
Производственная практика (по профилю специальности)		**36**

Виды работ: - участие в инсталляции и настройке регламентов обеспечения безопасности методами шифрования - участие в инсталляции сети и сетевых ресурсов, настройке регламентов обеспечения безопасности - установление маршрута согласований внутренних документов, а также участие в мероприятиях по переустановке, замене, переконфигурировании локальной сети в процессе эксплуатации автоматизированной системы - планирование и проектирование внутренних нормативных документов, а также участие в мероприятиях по введению и/или обновлению локальной сети в эксплуатацию - участие в организации работ по эксплуатации подсистем и средств безопасности локальной сети - ознакомление с особенностями функционирования систем обеспечения сетевой безопасности организации - оформление технической и технологической документации - участие в инсталляции сетевой БД и настройке регламентов обеспечения безопасного доступа	
Всего:	**466**

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 - ознакомительный (узнавание ранее изученных объектов, свойств);
2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Требования к материально-техническому обеспечению

Реализация профессионального модуля предполагает наличие лаборатории «Систем и сетей передачи»

Оборудование лаборатории «Систем и сетей передачи»:

- сетевой компьютерный класс;
- выделенный файл-сервер;
- выделенный сервер БД;
- комплект учебно-методической документации;
- наглядные пособия;
- специальное сетевое программное обеспечение;
- сетевой принтер;
- компьютерное рабочее место преподавателя;
- интерактивная доска;
- проектор;
- доступ в глобальные компьютерные сети.

Реализация программы модуля предполагает обязательную учебную практику, которую рекомендуется проводить рассредоточено, а также обязательную производственную практику, которую рекомендуется проводить концентрированно.

3.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1 Васильков А.В., и др. Информационные системы и их безопасность : учеб. пособие / А.В. Васильков. – М. : Форум, 2014. – 280 с.

2 Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах : учеб. пособие / А.В. Васильков, И.А. Васильков. – М. : Форум, 2014. – 250 с.

3 Васильков А.В. и др. Информационные системы и их безопасность : метод. пособие / А.В. Васильков. – М. : УМЦ ПО ДОМ, 2014. – 180 с.

4 Максимов Н.В., Попов И.И. Компьютерные сети: учебное пособие для студентов учреждений среднего профессионального образования. / Н.В. Максимов, И.И. Попов – 3-е изд., испр. и доп. – М.: Форум, 2014.- 350 с.

Дополнительная литература:

1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.

2. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2012. – 224 с.

3. ГубенковА.А.Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2012. - 88 с.

4. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2012

5. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2013.- 531 с.

6. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2012. – 656 с.

7. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2013.- 147 с.

8. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2012. – 240 с.

9. Руссинович М., Соломон Д., Внутреннее устройство MicrosoftWindows. Основные подсистемы операционной системы – Питер, 2014. – 672 с.

10. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2012. – 368 с.

Интернет - ресурсы:

1 Единое окно доступа к образовательным ресурсам [Электронный ресурс]. - Режим доступа: http://window.edu.ru

2 Федеральный центр информационно-образовательных ресурсов [Электронный ресурс]. - Режим доступа: http://fcior.edu.ru

2 SecurityLab by Positive Technologies [Электронный ресурс]. - Режим доступа: http://www.securitylab.ru/

3 Информационная безопасность [Электронный ресурс]. - Режим доступа: http://www.securrity.ru/

3.3. Организация образовательного процесса

Обучение по данному модулю основывается на знаниях и умениях, полученных при изучении общепрофессиональных дисциплин: Основы информационной безопасности;Технические средства информатизации; Организационно-правовое обеспечение информационной безопасности;Сети и системы передачи данных;Операционные системы; Базы данных.

Обучение по модулю проводится в виде лекционных и практических занятий. Практические занятия проводятся в компьютерных классах и лабораториях, оснащенных соответствующим программным обеспечением и ла-

бораторными установками. Время на изучение модуля – 364 часа, из них 114 часов практических занятий. В ходе проведения учебной практики студенты получают практические навыки по радиомонтажу. Время на отработку практических занятий в период учебной практики – 72 часа. В ходе проведения производственной практики студенты получают практические навыки согласно профессиональных компетенций, установленных ФГОС.

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках профессионального модуля «Эксплуатация автоматизированных информационых систем» является освоение МДК1 «Эксплуатация подсистем безопасности автоматизированных систем», МДК2 «Эксплуатация компьютерных сетей» и учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля.

Практика представляет собой вид учебных занятий, обеспечивающих практико-ориентированную подготовку обучающихся. При реализации профессионального модуля предусматриваются следующие виды практик: учебная и производственная (по профилю специальности).

Учебная практика проводится в лаборатории «Систем и сетей передачи» рассредоточено.

Производственная практика (по профилю специальности) проводится концентрированно по окончании изучения модуля.

Производственная практика проводится на предприятиях, в организациях, направление деятельности которых соответствует профилю подготовки обучающихся.

Аттестация по итогам производственной практики проводится с учетом результатов, подтвержденных документами соответствующих организаций.

Итоговая аттестация по профессиональному модулю «Эксплуатация автоматизированных информационных систем» проводится в форме экзамена (квалификационный) и предполагает обязательное наличие положительной аттестации по междисциплинарным курсам, учебной и производственной практикам (по профилю специальности) в рамках модуля.

3.4. Кадровое обеспечение образовательного процесса

К педагогической деятельности в Техникуме допускаются лица, имеющие высшее образование, отвечающие требованиям квалификационных характеристик, определенных для соответствующих должностей педагогических работников. Образовательный ценз указанных лиц подтверждается документами государственного образца о соответствующем уровне образования и (или) квалификации.

4. Контроль и оценка результатов освоения профессионального модуля (по разделам)

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	- точность и скорость диагностики нарушений эксплуатационных характеристик компонентов подсистем безопасности автоматизированных систем; - качество анализа эксплуатационных свойств компонентов подсистем безопасности автоматизированных систем, исходя из их служебного назначения; - качество рекомендаций по повышению эксплуатационных свойств компонентов подсистем безопасности автоматизированных систем; - выбор технологического оборудования, технических и организационных решений; - точность и грамотность оформления организационной и эксплуатационной документации	*Текущий контроль в форме:* *- защиты практических занятий;* *- контрольных работ.* *Зачеты по учебной практике и по разделу профессионального модуля.* *Дифференцированный зачёт по профессиональному модулю.*
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	- точность и скорость диагностики нарушений эксплуатационных характеристик систем; - качество анализа эксплуатационных свойств системы, исходя из ее служебного назначения; - качество принятия организационных решений по устранению прецедентов нарушения режимной эксплуатации; - качество рекомендаций по повышению безопасности эксплуатации системы; - выбор технологического оборудования, технических и организационных решений для решения задач по администрированию подсистем безопасности автоматизированных систем; - точность и грамотность оформления организационной и эксплуатационной документации	
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) си-	- обеспечение бесперебойной работы автоматизированных (информационных) систем в защищенном ис-	

стем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	полнении в соответствии с требованиями эксплуатационной документации - качество решений по организации мероприятий бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении	
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	- точность и скорость диагностики нарушений эксплуатационных характеристик систем; - качество анализа эксплуатационных свойств системы, исходя из ее служебного назначения; - качество рекомендаций по повышению эксплуатационных свойств системы; - выбор технологического оборудования, технических и организационных решений; - точность и грамотность оформления организационной и эксплуатационной документации	

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

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК.1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- выбор и применение методов и способов решения профессиональных задач в области эксплуатации компонент подсистемы безопасности автоматизированных систем; - оценка эффективности и качества выполнения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК.2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- эффективный поиск необходимой информации; - использование различных источников, включая электронные пособия	- наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики
ОК.3. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация целеустремленности, самообразования и саморазвития	- наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики

ОК.4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- демонстрация позитивных коммуникативных навыков и социальной адаптации; - качество принятых организационных решений	- наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики; -экспертная оценка портфолио работ студента
ОК.9. Использовать информационно-коммуникационные технологии в профессиональной деятельности	- работа с автоматизированными информационными системами	- наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики; -экспертная оценка портфолио работ студента