ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАЛМЫЦКИЙ ФИЛИАЛ

УТВЕРЖДАЮ
И.о. директора филиала
_____ Э.Л. Пашнанов
«28» 04 2020 г.

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

квалификация – техник по защите информации

Элиста, 2020 г.

ОДОБРЕНА
Предметно-цикловой комиссией естественнонаучных и математических дисциплин

протокол № 7
от «22» 04 2020 г.

председатель предметно-цикловой комиссии
Катрикова Ц.Ю./_____

Разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

заместитель директора по учебно-методической работе
Новгородова В.В./_____

составитель:

_____ Хамуров С.Б., высшая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»

рецензенты:

_____ Пипенко В.В., первая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»

_____ Агеев С.С., заместитель начальника отдела обеспечения деятельности, противодействия коррупции кадров и защиты информации, Министерства финансов Республики Калмыкия

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить основной вид деятельности Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующие ему профессиональные и общие 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.

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное

	поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем в защищённом исполнении; – администрирования автоматизированных систем в защищенном исполнении; – эксплуатации компонентов систем защиты информации автоматизированных систем; – диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении
уметь	– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – 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; – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности
знать	– состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; – принципы построения, физические основы работы периферийных устройств;

	– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; – принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего – 573 часов, в том числе:

максимальной учебной нагрузки обучающегося – 357 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 238 часов;

самостоятельной работы обучающегося – 119 часов;

учебной и производственной (по профилю специальности) практики –216 часов, на промежуточную аттестацию по МДК – 12 часов, демонстрационный экзамен по профессиональному модулю – 12 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 1.1. ОК 1– ОК 10	МДК 01.01. Эксплуатация автоматизированных систем	183	122	40	–	36	72	61
ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 10	МДК 01.02. Эксплуатация компьютерных сетей	174	116	50	–	36	72	58
ПК 1.1-1.4	Учебная практика	72						
ПК 1.1-1.4	Производственная практика	144						
	Всего:	573	238	90	–	72	144	119

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	
Семестр 5			
МДК.01.01 Эксплуатация автоматизированных систем		**183/122**	
Раздел 1. Разработка защищенных автоматизированных (информационных) систем			
Тема 1.1. Основы информационных систем как объекта защиты.	**Содержание**	**9/6**	
	Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.	2	**1**
	Основные особенности современных проектов АИС. Электронный документооборот.	2	
	Тематика практических занятий и лабораторных работ	**2**	
	Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	2	
Тема 1.2. Жизненный цикл автоматизированных систем	**Содержание**	**6**	
	Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.		
	Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.		

	Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.		
	Тематика практических занятий и лабораторных работ	**2**	
	Разработка технического задания на проектирование автоматизированной системы		
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	**Содержание**	**4**	
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации		
	Понятие уязвимости угрозы. Классификация уязвимостей.		
	Тематика практических занятий и лабораторных работ	**8**	
	Категорирование информационных ресурсов		
	Анализ угроз безопасности информации		
	Построение модели угроз		
Тема 1.4. Основные меры защиты информации в автоматизированных системах	**Содержание**	**4**	
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.		
	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним		
	Семестр 6		
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	**Содержание**	**10**	
	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.		
	Ограничение программной среды. Защита машинных носителей информации		
	Регистрация событий безопасности		
	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.		
	Обнаружение (предотвращение) вторжений		
	Контроль (анализ) защищенности информации Обеспечение целостности информационной системы и информации		

	Обеспечение доступности информации		
	Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.		
	Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных		
	Резервное копирование и восстановление данных.		
	Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.		
Тема 1.6. Защита информации в распределенных автоматизированных системах	**Содержание**	**4**	
	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.		
Тема 1.7. Особенности разработки информационных систем персональных данных	**Содержание**	**6**	
	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.		
	Тематика практических занятий и лабораторных работ	**4**	
	Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.		
Раздел 2.Эксплуатация защищенных автоматизированных систем.			
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	**Содержание**	**6**	
	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.		
	Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.		
	Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении		
Тема 2.2.	**Содержание**	**6**	

Администрирование автоматизированных систем	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.		
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	**Содержание**	**6**	
	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.		
Тема 2.4. Защита от несанкционированного доступа к информации	**Содержание**	**8**	
	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.		
	Классификация автоматизированных систем. Требования по защите информации от НСД для АС		
	Требования защищенности СВТ от НСД к информации		
	Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ		
Промежуточная аттестация по МДК.01.01		**2**	
Тема 2.5. СЗИ от НСД	**Содержание**	**8**	
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.		
	Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.		
	Обеспечение целостности информационной системы и информации		

	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности		
	Тематика практических занятий и лабораторных работ	**20**	
	Установка и настройка СЗИ от НСД		
	Защита входа в систему (идентификация и аутентификация пользователей)		
	Разграничение доступа к устройствам		
	Управление доступом		
	Использование принтеров для печати конфиденциальных документов. Контроль печати		
	Настройка системы для задач аудита		
	Настройка контроля целостности и замкнутой программной среды		
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности		
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	**Содержание**	**4**	
	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.		
	Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации		
	Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении		
	Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам		
	Тематика практических занятий и лабораторных работ	**2**	
	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем		
Тема 2.7. Документация на защищаемую автоматизированную систему	**Содержание**	**2**	
	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.		
	Тематика практических занятий и лабораторных работ	**2**	

	Оформление основных эксплуатационных документов на автоматизированную систему.		
Примерная тематика самостоятельной работы при изучении МДК.01.01 1. Разработка концепции защиты автоматизированной (информационной) системы 2. Анализ банка данных угроз безопасности информации 3. Анализ журнала аудита ОС на рабочем месте 4. Построение сводной матрицы угроз автоматизированной (информационной) системы 5. Анализ политик безопасности информационного объекта 6. Изучение аналитических обзоров в области построения систем безопасности 7. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации			
Промежуточная аттестация по МДК.01.01		**2**	
МДК.01.02. Эксплуатация компьютерных сетей		**116**	
Семестр 5			
Раздел 1. Основы передачи данных в компьютерных сетях			
Тема 1.1. Модели сетевого взаимодействия	**Содержание**	**2**	
	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.		
	Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.		
	Тематика практических занятий и лабораторных работ	**2**	
	Изучение элементов кабельной системы.		
Тема 1.2. Физический уровень модели OSI	**Содержание**	**2**	
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.		
	Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.		
	Оптоволоконные линии связи		
	Стандарты кабелей. Электрическая проводка.		
	Беспроводная среда передачи.		
	Тематика практических занятий и лабораторных работ	**2**	
	Создание сетевого кабеля на основе неэкранированной витой пары (UTP)		
	Сварка оптического волокна		

Тема 1.3. Топология компьютерных сетей	**Содержание**	**2**	
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий**.**		
	Тематика практических занятий и лабораторных работ	**4**	
	Разработка топологи сети небольшого предприятия		
	Построение одноранговой сети		
Тема 1.4. Технологии Ethernet	**Содержание**	**2**	
	Обзор технологий построения локальных сетей.		
	Технология Ethernet. Физический уровень.		
	Технология Ethernet. Канальный уровень		
	Тематика практических занятий и лабораторных работ	**2**	
	Изучение адресации канального уровня. MAC-адреса.		
Тема 1.5. Технологии коммутации	**Содержание**	**2**	
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI.		
	Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.		
	Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети		
	Технология PoweroverEthernet		
Тема 1.6. Сетевой протокол IPv4	**Содержание**	**10**	
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.		
	Маршрутизация пакетов IPv4		
	Протоколы динамической маршрутизации		
Тема 1.7. Скоростные и беспроводные сети	**Содержание**	**2**	
	Сеть FDDI. Сеть 100VG-AnyLAN Сверхвысокоскоростные сети Беспроводные сети		
Семестр 6			
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet			
Тема 2.1. Основы коммутации	**Содержание**	**2**	
	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах.		

	Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов		
	Тематика практических занятий и лабораторных работ	**2**	
	Работа с основными командами коммутатора.		
Тема 2.2. Начальная настройка коммутатора	**Содержание**	**2**	
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.		
	Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.		
	Тематика практических занятий и лабораторных работ	**4**	
	Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов		
	Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы		
Тема 2.3. Виртуальные локальные сети (VLAN)	**Содержание**	**8**	
	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.		
	Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation		
	Тематика практических занятий и лабораторных работ	**6**	
	Настройка VLAN на основе стандарта IEEE 802.1Q		
	Настройка протокола GVRP.		
	Настройка сегментации трафика без использования VLAN		
	Настройка функции Q-in-Q (Double VLAN).		
	Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.		
Тема 2.4. Функции повышения надежности и производительности	**Содержание**	**2**	
	Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.		
	Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.		
	Дополнительные функции защиты от петель. Агрегирование каналов связи.		
	Тематика практических занятий и лабораторных работ	**4**	
	Настройка протоколов связующего дерева STP, RSTP, MSTP.		
	Настройка функции защиты от образования петель LoopBackDetection		

	Агрегирование каналов.		
Тема 2.5. Адресация сетевого уровня и маршрутизация	**Содержание**	**8**	
	Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.		
	Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.		
	Планирование подсетей IPv6. Протокол NDP.		
	Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.		
	Тематика практических занятий и лабораторных работ	**6**	
	Основные конфигурации маршрутизатора.		
	Расширенные конфигурации маршрутизатора.		
	Работа с протоколом CDP.		
	Работа с протоколом TELNET. Работа с протоколом TFTP.		
	Работа с протоколом RIP.		
	Работа с протоколом OSPF.		
	Конфигурирование функции маршрутизатора NAT/PAT.		
	Конфигурирование PPP и CHAP.		
Тема 2.6. Качество обслуживания (QoS)	**Содержание**	**4**	
	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.		
	Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.		
	Тематика практических занятий и лабораторных работ	**2**	
	Настройка QoS. Приоритизация трафика. Управление полосой пропускания		
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	**Содержание**	**2**	
	Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.		
	Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.		
	Тематика практических занятий и лабораторных работ	**2**	
	Списки управления доступом (AccessControlList)		
	Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.		
	Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding		

Тема 2.8. Многоадресная рассылка	**Содержание**	**2**	
	Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.		
	Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping).Функция IGMP FastLeave.		
	Тематика практических занятий и лабораторных работ	**4**	
	Отслеживание трафика многоадресной рассылки.		
	Отслеживание трафика Multicast		
Тема 2.9. Функции управления коммутаторами	**Содержание**	**2**	
	Управление множеством коммутаторов. Протокол SNMP.		
	RMON (Remote Monitoring). Функция Port Mirroring.		
	Тематика практических занятий и лабораторных работ	**4**	
	Функции анализа сетевого трафика.		
	Настройка протокола управления топологией сети LLDP.		
Раздел 3. Межсетевые экраны			
Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	**Содержание**	**6**	
	Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.		
	Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.		
Тема 3.2. Межсетевые экраны	**Содержание**	**2**	
	Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.		
	Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.		
	Тематика практических занятий и лабораторных работ	**4**	
	Основы администрирования межсетевого экрана		
	Соединение двух локальных сетей межсетевыми экранами		
	Создание политики без проверки состояния.		
	Создание политик для традиционного (или исходящего) NAT.		
	Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing		
Тема 3.3. Системы обнаружения	**Содержание**	**2**	
	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные		

и предотвращения проникновений	инструментальные средства.		
	Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.		
	Тематика практических занятий и лабораторных работ	**2**	
	Обнаружение и предотвращение вторжений.		
Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	**Содержание**	**2**	
	Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.		
Примерная тематика самостоятельной работы при изучении МДК.01.02 1. Физическое кодирование с использованием манчестерского кода 2. Логическое кодирование с использованием скремблирования 3. Подключение клиента к беспроводной сети в инфраструктурном режиме 4. Оценка беспроводной линии связи 5. Проектирования беспроводной сети 6. Сбор информации о клиентских устройствах 7. Планирование производительности и зоны действия беспроводной сети 8. Предпроектное обследование места установки беспроводной сети 9. Обеспечение отказоустойчивости в беспроводных сетях 10. Режимы работы и организация питания точек доступа 11. Сегментация беспроводной сети 12. Настройка QoS 13. Постпроектное обследование и тестирование сети 14. Создание ACL-списка 15. Наблюдение за трафиком в сети VLAN 16. Определение уязвимых мест сети 17. Реализация функций обеспечения безопасности порта коммутатора 18. Исследование трафика 19. Создание структуры сети организации 20. Определение технических требований 21. Мониторинг производительности сети 22. Создание диаграммы логической сети			

23. Подготовка к обследованию объекта 24. Обследование зоны беспроводной связи 25. Формулировка общих целей проекта 26. Разработка требований к сети 27. Анализ существующей сети 28. Определение характеристик сетевых приложений 29. Анализ сетевого трафика 30. Определение приоритетности трафика 31. Изучение качества обслуживания сети 32. Исследование влияния видеотрафика на сеть 33. Определение потоков трафика, построение диаграмм потоков трафика 34. Определение проектных стратегий для достижения масштабируемости 35. Определение стратегий повышения доступности 36. Определение требований к обеспечению безопасности 37. Разработка ACL-списков для реализации наборов правил межсетевого экрана 38. Использование CIDR для обеспечения объединения маршрутов 39. Определение схемы IP-адресации 40. Определение количества IP-сетей 41. Создание таблицы для выделения адресов 42. Составление схемы сети 43. Анализ плана тестирования и выполнение теста 44. Создание плана тестирования для сети комплекса зданий 45. Проектирование виртуальных частных сетей 46. Безопасная передача данных в беспроводных сетях		
Примерные виды самостоятельных работ при изучении раздела 2 модуля 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 практических работ, отчетов к их защите.		
Учебная практика раздела 2 модуля **Виды работ** 1. Проведение аудита защищенности автоматизированной системы. 2. Установка, настройка и эксплуатация сетевых операционных систем. 3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной	*72*	

системы. 4. Организация работ с удаленными хранилищами данных и базами данных. 5. Организация защищенной передачи данных в компьютерных сетях. 6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. 7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. 8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.		
Производственная практика **Виды работ:** 1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения 3. Настройка программного обеспечения с соблюдением требований по защите информации 4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам 5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением 6. Настройка встроенных средств защиты информации программного обеспечения 7. Проверка функционирования встроенных средств защиты информации программного обеспечения 8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения 9. Обслуживание средств защиты информации в компьютерных системах и сетях 10. Обслуживание систем защиты информации в автоматизированных системах 11. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем 12. Проверка работоспособности системы защиты информации автоматизированной системы 13. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации 14. Контроль стабильности характеристик системы защиты информации автоматизированной системы 15. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем 16. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	**144**	
Экзамен по профессиональному модулю (демонстрационный экзамен)	**12**	
Всего	**573**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебного кабинета, лабораторий Информационных технологий, программирования и баз данных, Сетей и систем передачи информации, Программных и программно-аппаратных средств защиты информации, мастерских «Корпоративная защита от внутренних угроз информационной безопасности», «Анализ защищённости информационных систем от внешних угроз».

Оборудование учебного кабинета и рабочих мест кабинета Информатики, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

Оборудование лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами (Proceccor: Intel Core i5, частота не менее 2,4 ГГц, поддержка памяти DDR4 до 128 ГБ, ОЗУ DIMM, DDR4 не менее 8 Гб; HDD не менее 500 Гб; SSD не менее 400Гб);
- лабораторные учебные макеты;
- рабочее место преподавателя (Proceccor: Intel Core i5, частота не менее 2,4 ГГц, поддержка памяти DDR4 до 128 ГБ, ОЗУ DIMM, DDR4 не менее 8 Гб; HDD не менее 500 Гб; SSD не менее 400Гб);
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности (ПО для защиты от утечек типа InfoWatch Traffic Monitor 6.9 или аналог, InfoWatch Device Monitor 6.9 или аналог, InfoWatch Crawler 1.4 или аналог, соответствующие лицензии на весь период проведения , БД PostgreSQL 9.5 (под Windows) или функциональный аналог);
- программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей (Защита конечных точек Secret Net Studio, Соболь, Terminal, Защита сети АПКШ «Континент», Сервер доступа «Континент» и СКЗИ «Континент-АП»);
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации (Крипто-Про).

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники

1. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры: учебник для студ. учреждений сред. проф. образования - издательский центр «Академия», 2020 г. – 288 с.
2. Бубнов А.А., Пржегорлинский В.Н., Фомина К.Ю. Техническая защита информации в объектах информационной инфраструктуры: учебник для студ. учреждений сред. проф. образования/– М.: Издательский центр «Академия», 2019 -272 с.
3. Кравченко В.Б., Зиновьев П.В., Селютин И.Н Эксплуатация автоматизированных (информационных) систем в защищенном исполнении: учебник для студ. учреждений сред. проф. образования/ – М.: Издательский центр «Академия», 2018 - 304 с.
4. Кравченко В.Б. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении: учеб. пособие для студ. учреждений сред проф. образования/ В,Б.Кравченко, П.В. Зиновьев, И.Н. Селютин.- М.: Издательский центр «Академия», 2018.- 304с.
5. Гагарина Л.Г., Киселев Д.В., Федотова Е.Л. Разработка и эксплуатация автоматизированных информационных систем: учеб пособие/ Под ред. Проф. Л.Г. Гагариной.- М.: ИД «ФОРУМ» ИНФРА-М,2007.-384с.- (Профессиональное образование).
6. Максимов Н.В., Попов И.И. Компьютерные сети: учебное пособие/ Н.В. Максимов, И.И.Попов.-4-е изд., перераб. и доп.- М.:ФОРУМ,2011.-464с.-(Профессиональное образование).

3.2.2. Дополнительные печатные источники:

1. Гвоздева В.А., Лаврентьев И.Ю. Основы построения автоматизированных информационных систем: учебник.- М.: ИД «ФОРУМ» : ИНФРА-М,2009.-320с.- (Профессиональное образование)
2. Емельянова Н.З., Партыка Т.Л., Попов И.И. Основы построения автоматизированных информационных систем: учебное пособие,- М.: ФОРУМ: ИНФРА-М, 2005.-416с.- (Профессиональное образование)
3. Виснадул Б.Д., Лунин С.А, Сидоров С.В., Чумаченко П.Ю. Основы компьютерных сетей: учеб. пособие/ под ред. Л.Г. Гагариной.- М.: ИД «ФОРУМ»: ИНФРА-М,2007.-272 с.- (Профессиональное образование)
4. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2013

3.2.3. Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Журналы Защита информации. Инсайд: Информационно-методический журнал

3. Информационная безопасность регионов: Научно-практический журнал

4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.4. Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11. Федеральный портал «Российское образование www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ,

документации.	документации	оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанную преподавателем Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет» Хамуровым С.Б.

Представленная рабочая программа профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

Рецензируемая рабочая программа профессионального модуля имеет чёткую структуру и включает все необходимые компоненты.

В паспорте рабочей программы определена область применения программы, раскрываются цели, задачи модуля - требования к результатам освоения профессионального модуля.

Объем профессионального модуля, виды учебной работы, тематический план и содержание профессионального модуля раскрывают структуру и содержание профессионального модуля. Указанные объем часов максимальной, обязательной аудиторной учебной нагрузки, практических занятий, самостоятельной работы обучающихся и форма промежуточной аттестации соответствуют учебному плану. Виды самостоятельной работы позволяют привить обучающимся умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечить высокий уровень успеваемости в период обучения. В тематическом плане и содержании профессионального модуля раскрывается последовательность изучения разделов и тем программы, показываются распределение учебных часов по разделам, темам и указывается уровень освоения. Дидактические единицы, отраженные в содержании учебного материала, направлены на качественное усвоение учебного материала. Для приобретения практических навыков и повышения уровня знаний предусмотрены практические занятия.

Условия реализации профессионального модуля определяют требования к необходимому материально-техническому обеспечению к оборудованию учебной лаборатории и техническим средствам обучения. Информационное обеспечение обучения содержит современный перечень рекомендуемых учебных изданий, дополнительной литературы и интернет-ресурсов.

Контроль и оценка результатов освоения профессионального модуля содержит результаты обучения, формы и методы контроля и оценки результатов обучения, которые осуществляются преподавателем в процессе проведения различных форм учебных занятий.

Рецензируемая рабочая программа рекомендуется для реализации в образовательном процессе.

Рецензент Ипенко В.В., преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно- экономический университет»

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанную преподавателем Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет» Хамуровым С.Б.

Представленная рабочая программа профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении разработана с учетом требований Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования на основе Федеральных государственных образовательных стандартов СПО.

В паспорте рабочей программы определена область применения рабочей программы, сформулированы цели и задачи, требования к результатам освоения профессионального модуля.

Объем профессионального модуля и виды учебной работы, предусмотренные структурой профессионального модуля, соответствуют тематическому содержанию профессионального модуля.

Содержание программы направлено на приобретение обучающимися знаний, умений, направленных на формирование общих и профессиональных компетенций, определенных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и соответствует объему часов, указанному в рабочем учебном плане.

Материально-техническое обеспечение включает наличие учебной лаборатории, оснащенной оборудованием и техническими средствами обучения.

Информационное обеспечение обучения содержит перечень современных учебных изданий, дополнительной литературы и интернет-ресурсов.

Контроль и оценка результатов освоения профессионального модуля содержит профессиональные и общие, формы, методы контроля оценки результатов обучения и осуществляется преподавателем в процессе проведения различных форм учебных занятий.

Рабочая программа позволит студентам в достаточной мере освоить профессиональный модуль, овладеть общими и профессиональными компетенциями, необходимых для качественного освоения программы подготовки специалистов среднего звена.

Рабочая программа профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении рекомендуется к применению в учебном процессе Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет».

Рецензент _____ Агеев С.С., заместитель начальника отдела обеспечения деятельности, противодействия коррупции кадров и защиты информации, Министерства финансов Республики Калмыкия