МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Восточно-Сибирский государственный университет технологий и управления»

Технологический колледж

СОГЛАСОВАНО:
Зам. директора по УМР ТК ВСГУТУ
_____ В.В.Пойдонова

УТВЕРЖДАЮ:
Директор ТК ВСГУТУ
_____ С.Н.Сахаровский
«_25_» ___04___ 2018 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Эксплуатация объектов сетевой инфраструктуры

для студентов специальности 09.02.02 «Компьютерные сети»
(квалификация *техник по компьютерным сетям*)

Улан-Удэ
2018

Рабочая программа ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» разработана в технологическом колледже ВСГУТУ и является частью программы подготовки специалистов среднего звена (ППССЗ), разработанной в соответствии с федеральным государственным образовательным стандартом среднего общего образования, в соответствии с Рекомендациями по организации получения среднего общего образования в пределах освоения образовательных программ среднего профессионального образования на базе основного общего образования с учетом требований федеральных государственных образовательных стандартов и получаемой профессии или специальности среднего профессионального образования (письмо Департамента государственной политики в сфере подготовки рабочих кадров и ДПО Минобрнауки России от 17.03.2015 № 06-259).

Составители:

_____Алтаев А.А.

_____Литвинова М.А.

Рабочая программа рассмотрена, обсуждена и одобрена на заседании ЦМК по профессиональным дисциплинам.
Протокол от «03» 09 2018 г № 1

Председатель ЦМК _____ Литвинова М.А.

Восточно-Сибирский государственный университет технологий и управления
Технологический колледж

Рабочая программа профессионального модуля ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» для специальности 09.02.02 «Компьютерные сети»

Аннотация

1. Место дисциплины в учебно-воспитательном процессе

Дисциплины относится к профессиональному модулю учебного плана ППССЗ, реализуется на 3 и 4-ом годах обучения (6 и 7 семестры).

2. Цели изучения и планируемые результаты освоения дисциплины

В результате освоения дисциплины у обучающихся должны быть сформированы следующие компетенции: ОК 1; ОК 2; ОК 3; ОК 4; ОК 5; ОК 6; ОК 7; ОК 8; ОК 9; ПК 3.1; ПК 3.2; ПК 3.3; ПК 3.4; ПК 3.5; ПК 3.6 (ФГОС СПО № 827 от 28.07.2014г. пп 5, 6).

В результате изучения обязательной части учебного цикла обучающийся должен **уметь**:

- иметь практический опыт:
- обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;
- удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;
- организации бесперебойной работы системы по резервному копированию и восстановлению информации;
- поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры;
- уметь:
- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры;
- осуществлять диагностику и поиск неисправностей технических средств;
- выполнять действия по устранению неисправностей в части, касающейся полномочий техника;
- тестировать кабели и коммуникационные устройства;
- выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;
- правильно оформлять техническую документацию;

В результате изучения обязательной части учебного цикла обучающийся должен **знать**:

- архитектуру и функции систем управления сетями, стандарты систем управления;
- задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;
- средства мониторинга и анализа локальных сетей;
- классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;
- правила эксплуатации технических средств сетевой инфраструктуры;
- расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;

- методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных.

3. Структура и содержание дисциплины

Структура дисциплины:

Вид учебной работы	*Объём часов*
Максимальная учебная нагрузка	*251*
Обязательная аудиторная учебная нагрузка (всего)	*170*
в том числе:	
практические занятия	*85*
Самостоятельная работа обучающегося (всего)	*79*
в том числе:	
Консультации	*2*
Промежуточная аттестация	*ДЗ*

Содержание дисциплины: Физические и логические (информационные) аспекты эксплуатации, расширяемость и масштабируемость сети, техническая и проектная документация.

4. Список авторов профессионального модуля.

Алтаев А.А., доцент кафедры Систем информатики ВСГУТУ,

Литвинова М.А., старший преподаватель кафедры Электронно-вычислительных систем ВСГУТУ.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры»

1.1. Область применения программы

Рабочая программа профессионального модуля является частью ППССЗ в соответствии с ФГОС СПО специальности 09.02.02 «Компьютерные сети» от 28 июля 2014 г. № 803.

1.2. Место дисциплины в структуре основной образовательной программы:

Профессиональный модуль дисциплин МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры» и МДК.03.02 «Безопасность функционирования информационных систем» относится к профессиональному модулю учебного плана специальности 09.02.02 «Компьютерные сети».

Компетенции, формируемые в результате освоения содержания профессионального модуля ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» необходимы для успешной подготовки выпускной квалификационной работы.

1.3. Цели изучения и планируемые результаты освоения дисциплины

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся, в ходе освоения профессионального модуля, должен **иметь практический опыт:**

– обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;

– удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;

– организации бесперебойной работы системы по резервному копированию и восстановлению информации;

– поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры;

уметь:

– выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;

– использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры;

– осуществлять диагностику и поиск неисправностей технических средств;

– выполнять действия по устранению неисправностей в части, касающейся полномочий техника;

– тестировать кабели и коммуникационные устройства;

– выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;

– правильно оформлять техническую документацию;

– наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;

– устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;

знать:

– архитектуру и функции систем управления сетями, стандарты систем управления;

– задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;

– средства мониторинга и анализа локальных сетей;

– классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;

– правила эксплуатации технических средств сетевой инфраструктуры;

– расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;

– методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;

– основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем (ИС), требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;

– основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

В результате освоения дисциплины у обучающихся формируются следующие профессиональные компетенции:

Код	Профессиональные компетенции
ПК 3.1.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей
ПК 3.2.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях
ПК 3.3.	Эксплуатация сетевых конфигураций
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации
ПК 3.5.	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта
ПК 3.6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры

Освоение дисциплины направлено на формирование и развитие общих компетенций:

Код	Общие компетенции
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы решения профессиональных задач, оценивать их эффективность и качество
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4.	Осуществлять поиск и использование информации. Необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Распределение учебного времени модуля

Распределение учебного времени выполнено в виде выписки из УП. В таблице 1 представлена информация по каждой форме обучения о распределении общей трудоемкости обучения в часах по семестрам, видов и объемов учебной работы в часах (лекции (Л)), практические занятия (Пр), о распределении форм СРС – самостоятельной работы студентов, расчетно-графические работы (РГР), контрольные (КР) и другие работы), а также форм ПА – промежуточной аттестации студентов по дисциплине(экзамен (Э), дифференцированный зачет (ДЗ), зачет (З), другие формы контроля):

Таблица 1 – Распределение учебного времени дисциплины

Форма обучения	Наименование разделов ПМ	Семестр и его продолжительность (нед.)	РАСПРЕДЕЛЕНИЕ							
			Максимальная нагрузка (час)	В том числе					Форм СРС	Форм ПА - аттестация
				На аудиторные занятия (час)			на СРС (час)	Конс (час)		
				Всего (час)	В том числе					
					Л (час)	Пр (час)				
Очная	МДК 03.01. Эксплуатация объектов сетевой инфраструктуры	4 год, 1 семестр 16 нед 4 год, 2 семестр 18 нед	251	170	85	85	79	2	ИЗ1 ИЗ2	ДЗ
	МДК 03.02. Безопасность функционирования информационных систем	4 год, 1 семестр 16 нед 4 год, 2 семестр 18 нед	201	136	68	68	65			ДЗ
	Учебная практика		36							ДЗ
	Производственная практика		180							ДЗ
	Итого		**668**	**306**	**153**	**153**	**144**	**2**		

2.2. Тематический план и содержание учебной дисциплины

Таблица 2.

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем		Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1		2	3	4
ПМ 03. Эксплуатация объектов сетевой инфраструктуры			**452**	
МДК 03.01 Эксплуатация объектов сетевой инфраструктуры			251	
Введение		Объекты сетевой инфраструктуры и их эксплуатация	**2**	
Раздел 1. **Эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей.**			**14**	
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры	**Содержание**		4	
	1.	**Физические аспекты эксплуатации.** Физическое вмешательство в инфраструктуру сети; активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.		2
	2.	**Логические (информационные) аспекты эксплуатации.** Несанкционированное ПО (в том числе сетевое); паразитная нагрузка.		2
	3.	**Расширяемость сети. Масштабируемость сети.** Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб); наращивание длины сегментов сети; замена существующей аппаратуры (на более мощную). Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.		3
	4.	**Техническая и проектная документация.** Паспорт технических устройств; руководство по эксплуатации; Физическая карта всей сети; логическая схема компьютерной сети;		1
	Практические занятия		4	
	1	Поддержка пользователей сети.		
	2	Создание пользователей в domain, редактирование пользователей в domain, создание пароля пользователем в domain, создание групп и распределение пользователей по группам в domain.		
	3	Настройка прав доступа.		
	4	Оформление технической документации, правила оформления документов.		
	5	Настройка аппаратного и программного обеспечения сети. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.		

Самостоятельная работа обучающихся по разделу 1: Повторение пройденного материала; Примерная тематика внеаудиторной работы: Физическая инфраструктура; Логическая инфраструктура; Сетевые подключения, протоколы, адресация, система имен. Автоматическое назначение частных IP-адресов; Маршрутизация и инфраструктура сети Windows Server 2012; Установка сетевых компонентов Windows; Установка Active Directory в сети Windows; Разбиение на подсети; Механизм разбиения на подсети; Определение емкости подсети;			6	
Раздел 2. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях.			**11**	
Тема 2.1 Профилактические работы	**Содержание**		6	2
	1.	**Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры** Комплекс организационно-технических мероприятий; выявление и своевременная замена элементов инфраструктуры.		
	2.	**Проверка объектов сетевой инфраструктуры и профилактические работы** Проверка физических компонентов; проверка документации и требований; проверка списка совместимого оборудования.		3
	3.	**Проведение регулярного резервирования** Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения.		2
	Практические занятия		2	
	1.	Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.		
	2.	Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы, коммутационное оборудование)		
Самостоятельная работа обучающихся по разделу 1: **Примерная тематика внеаудиторной самостоятельной работы:** Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. Технические регламенты, виды документов для технических осмотров, методы и принципы проверки различного оборудования, методы резервирования, программы для резервирования информации, BackUp. Маршрутизация в Windows Server 2003; Управление общими свойствами IP-маршрутизации; Основные сведения о NAT; Различие между NAT и ICS; Удаленный доступ по телефонной линии; Авторизация подключений удаленного доступа.			3	

Раздел 3. Эксплуатация сетевых конфигураций.			**49**	
Тема 3.1 Управление сетями	**Содержание**		14	2
	1.	**Архитектура системы управления. Структура системы управления.** Архитектура в концепции TMN; централизованное управление; децентрализованное управление.		
	2.	**Уровни управления** Многоуровневая архитектура управления TMN: бизнесом; услугами; сетью; элементами сети; уровень элементов сети.		2
	3.	**Области управления.** Области управления ошибками; конфигурацией; доступом; производительностью; безопасностью.		2
	4.	**Протоколы управления.** SNMP; CMIP; TMN; LNMP; ANMP.		2
	5.	**Управление отказами.** Выявление, определение и устранение последствий сбоев и отказов в работе сети.		2
	6.	**Учет работы сети. Управление конфигурацией.** Регистрация, управление используемыми ресурсами и устройствами; конфигурирование компонентов сети, сетевые адреса и идентификаторы, управление параметрами сетевых операционных систем.		3
	7.	**Управление производительностью, безопасностью сети.** Статистика работы сети в реальном времени, минимизации заторов и узких мест, выявления складывающихся тенденций и планирования ресурсов для будущих нужд; Контроль доступа, сохранение целостности данных и журналирование.		3
	Практические занятия		4	
	1	Анализ сетевого трафика средствами Сетевого монитора		
	2	Основные сведения о сетевом мониторе		
	3	Запись данных средствами Сетевого монитора		
	4	Устранение неполадок с помощью Ping и PathPing		
	5	Диагностика сети и Netdiag		
	6	Удаленное администрирование;		
	7	Восстановление работоспособности сетевой инфраструктуры.		
	8	Авторизация подключений удаленного доступа		
Тема 3.2 Средства	**Содержание**		8	2

мониторинга и анализа локальных сетей	1.	**Анализаторы протоколов** Программные или аппаратно-программные системы, функции мониторинга, анализ трафика в сетях.		
	2.	**Оборудование для диагностики и сертификации кабельных систем** Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.		2
	3.	**Экспертные системы** Выявление причин аномальной работы сетей; возможные способы приведения сети в работоспособное состояние.		3
	4.	**Встроенные системы диагностики и управления. Сетевые мониторы** Средняя интенсивность общего трафика сети, средняя интенсивность потока пакетов с определенным типом ошибки. Программно-аппаратный модуль, установленный в коммуникационное оборудование, программный модуль, встроенный в операционные системы.		2
	Практические занятия		7	
	1	Вкладка. Сеть утилиты. Диспетчер задач		
	2	Использование консоли. Производительность		
	3	Мониторинг сетевого трафика с помощью утилиты Netstat		
	4.	Тестирование кабелей		
	5	Тестирование коммутационного оборудования		
Самостоятельная работа обучающихся по разделу 3: Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** Основные сведения о политиках удаленного доступа Устранение неполадок при подключениях удаленного доступа Реализация процедур безопасного администрирования сети Оснастка Шаблоны безопасности Схемы обжимки витой пары; Устройство «пакета», передаваемого по сети. Использование бесклассовой междоменной маршрутизации; Маски подсети переменной длины; Проверка существующего IP-адреса; Ручная настройка адреса; DNS; NetBIOS; DNS в сетях Windows Server 2003; Механизм работы DNS-запросов; Настройка параметров DNS-сервера; Средства устранения неполадок DNS;			16	
Раздел 4. Схемы послеаварийного восстановления работоспособности компьютерной сети.			**80**	
Тема 4.1 Хранение	**Содержание**		12	3

информации	1.	**Резервное копирование данных**		
	2.	**Хранилища данных** Принципы работы хранилищ данных. Принципы построения. Основные компоненты хранилища данных		2
	3.	**Технологии управления информацией. OLAP-технология**		2
	4.	**Понятие баз данных.** Основные понятия, принцип работы. СУБД		3
	Практические занятия		16	
	1.	Операции по резервному копированию данных;		
	2.	Операции по восстановлению данных.		
	3.	Организации по бесперебойной работе системы по резервному копированию		
	4.	Восстановление информации		
Тема 4.2 Схема после аварийного восстановления	**Содержание**		12	
	1.	Принципы планирования восстановления работоспособности сети при аварийной ситуации		2
	2.	Допущения при разработке схемы послеаварийного восстановления. Основные требования к политике организации схемы послеаварийного восстановления		2
	3.	Организация работ по восстановлению функционирования системы		2
	4.	**План восстановления системы** Порядок уведомления о чрезвычайных событиях. Активация. Возврат к нормальному функционированию системы.		3
	Практические занятия		16	
	1.	Восстановление работоспособности сети после сбоя		
	2.	Разработка плана восстановления		
	3.	Использовать схему после аварийного восстановления сети.		
	4.	Возврат к нормальному функционированию системы.		
Самостоятельная работа обучающихся по разделу 4: Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** Повторение пройденного материала, Изучение утилиты Acronis, изучение безопасной зоны Acronis, Создание контрольной точки восстановления с помощью Acronis;			24	

Создание базы данных на примере учебной группы; Разработка плана восстановления работоспособности сети на примере одной взятой организации (колледжа, офиса)				
Раздел 5.	**Замена расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры.**		**89**	
Тема 5.1. Диагностика неисправностей технических средств и сетевой структуры	**Содержание**		27	
	1.	Принципы локализации неисправностей		3
	2.	Контрольно-измерительная аппаратура		3
	3.	Сервисные платы и комплексы		3
	4.	Программные средства диагностики		2
	5.	Номенклатура и особенности работы тест-программ		2
	6.	Диагностика неисправностей средств сетевых коммуникаций		3
	7.	Контроль функционирования аппаратно-программных комплексов.		2
	8.	Действия при не работающей сети, при медленной сети,		3
	9.	Действия при не стабильно работающей сети.		3
	Практические занятия		32	
	1.	Работа контрольно-измерительной аппаратуры		
	2.	Замена расходных материалов		
	3.	Мелкий ремонт периферийного оборудования		
	4.	Программная диагностика неисправностей		
	5.	Аппаратная диагностика неисправностей		
	6.	Поиск неисправностей технических средств		
	7.	Выполнение действий по устранению неисправностей		
	8.	Установка программного обеспечения		
Самостоятельная работа обучающихся по разделу 5: Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** Поиск неисправностей по принципу локализации неисправностей конкретного оборудования; Изучить и понять принцип работы новых контрольно-измерительных аппаратов			30	

МДК 03.02. Безопасность функционирования информационных систем			**251**	
Раздел 6.	**6 семестр. Темы 6.1 и 6.2**		**51**	
Введение	Информационная безопасность и технологии защиты информации		2	
Тема 6.1 Основы информационной безопасности	**Содержание**		6	**3**
	1.	**Понятие национальной безопасности.** Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.		
	2.	**Информационная безопасность в системе национальной безопасности Российской Федерации.** Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере.		**2**
	3.	**Государственная информационная политика.** Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.		**3**
	4.	**Информация - наиболее ценный ресурс современного общества.** Понятие «информационный ресурс». Классы информационных ресурсов.		**3**
	5.	**Проблемы информационной войны.** Информационное оружие и его классификация. Информационная война.		**3**
	6.	**Проблемы информационной безопасности в сфере государственного и муниципального управления.** Информационные процессы в сфере государственного и муниципального управления. Виды информации и информационных ресурсов в сфере ГМУ. Состояние и перспективы информатизации сферы ГМУ.		**3**
	7.	**Информационные системы.** Общие положения. Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах.		**3**
	8.	**Методы и модели оценки уязвимости информации.** Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита»		**3**
	Практические занятия		8	
	1.	Установка программы Ethereal и подготовка к захвату.		
	2.	Пользовательский интерфейс программы Ethereal. Фильтр отображения пакетов. Поиск кадров.		
	3.	Выделение ключевых кадров. Сохранение данных захвата. Печать информации.		

		Просмотр кадра в отдельном окне.		
	4.	Анализ протоколов Ethernet и ARP.		
	5.	Анализ протоколов IP и ICMP.		
	6.	Анализ протокола TCP		
Тема 6.2. Проблемы информационной безопасности.	**Содержание**		8	**3**
	1.	**Основные понятия и анализ угроз информационной безопасности.** Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.		
	2.	**Проблемы информационной безопасности сетей.** Введение в сетевой информационный обмен. Анализ угроз сетевой безопасности. Обеспечение информационной безопасности сетей.		**3**
	3.	**Политика безопасности.** Основные понятия политики безопасности. Структура политики безопасности организации.		**3**
	4.	**Стандарты информационной безопасности.** Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий		**3**
	Лабораторные работы		6	
	1.	Система анализа рисков проверки политики информационной безопасности предприятия.		
	2.	Анализ угроз сетевой безопасности.		
	3.	Обеспечение информационной безопасности сетей.		
	Практические занятия		6	
	1.	Этапы сетевой атаки. Исследование сетевой топологии.		
	2.	Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы		
	3.	Реализации атак. Выявление атаки на протокол SMB.		
Раздел 6.	**6 семестр. Темы 6.3 - 6.5**		**150**	
Тема 6.3. Технологии защиты данных.ё	**Содержание**		20	**2**
	1	**Принципы криптографической защиты информации.** Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированная криптосистема шифрования. Электронная цифровая подпись и функция хэширования.		

	2	**Криптографические алгоритмы.** Классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Асимметричные криптоалгоритмы.		**3**
	3	**Технологии аутентификации.** Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя.		**3**
	Лабораторные работы		20	
	1	**Изучение стандарта криптографической защиты AES (Advanced Encryption Standart).**		
	2	**Изучение отечественных стандартов хэш-функции и цифровой подписи.**		
Тема 6.4. Технологии защиты межсетевого обмена данными.	**Содержание**		**22**	
	1	**Обеспечение безопасности операционных систем.** Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС.		**2**
	2	**Технологии межсетевых экранов.** Функции межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе МЭ.		**3**
	3	**Основы технологии виртуальных защищенных сетей VPN.** Концепция построения виртуальных защищенных сетей VPN. VPN-решения для построения защищенных сетей. Достоинства применения технологий VPN.		**2**
	4	**Защита на канальном и сеансовом уровнях.** Протоколы формирования защищенных каналов на канальном уровне. Протоколы формирования защищенных каналов на сеансовом уровне. Защита беспроводных сетей.		**3**
	5	**Защита на сетевом уровне - протокол IPSEC.** Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол управления криптоключами IKE. Особенности реализации средств IPSec.		**2**
	6	**Инфраструктура защиты на прикладном уровне.** Управление идентификацией и доступом. Организация защищенного удаленного доступа. Управление доступом по схеме однократного входа с авторизацией Single Sign-On. Протокол Kerberos. Инфраструктура управления открытыми ключами PKI.		**1**
	Практические занятия		18	
	1	**Компоненты межсетевого экрана. Политика межсетевого экранирования**		
	2	**Архитектура МЭ. Пример реализации политики МЭ.**		

	3.	**Применение МЭ на основе двудомного узла. Применение МЭ на основе фильтрующего маршрутизатора. Применение МЭ на основе экранирующего узла**		
	4.	**Применение технологии трансляции сетевых адресов.**		
	5.	**Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.**		
	6.	**Организация VPN средствами протокола PPTP. Защита данных на сетевом уровне**		
	7.	**Организация VPN средствами СЗИ VipNet. Использование протокола IPSec для защиты сетей.**		
	8.	**Организация VPN средствами СЗИ StrongNet. Защита на транспортном уровне**		
	9.	**Организация VPN средствами протокола SSL в Windows Server**		
Тема 6.5. Технологии обнаружения вторжений.	**Содержание**		8	
	1	**Анализ защищенности и обнаружение атак.** Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак.		**1**
	2	**Защита от вирусов. Методы управления средствами сетевой безопасности.** Компьютерные вирусы и проблемы антивирусной защиты. Антивирусные программы и комплексы. Построение системы антивирусной защиты корпоративной сети. Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности.		**3**
	Практические занятия		12	
	1.	**Сигнатурный анализ и обнаружение аномалий**		
	2.	**Обнаружение в реальном времени и отложенный анализ.** Локальные и сетевые системы обнаружения атак		
	3.	**Распределенные системы обнаружения атак.** Система обнаружения атак Snort.		
Самостоятельная работа при изучении раздела ПМ 03 раздела 6 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** Службы каталогов. Подготовка индивидуального задания по теме «Аудит информационной безопасности компьютерных систем».			**65**	

Учебная практика (по профилю специальности) ПМ.03	**36**	
Производственная практика (по профилю специальности) ПМ.03	**180**	
Виды работ: Использование активного и пассивного оборудования сети. Устранение паразитирующей нагрузки в сети. Заполнение технической документации. Построение физической карты локальной сети. Работа по созданию, редактированию, удалению пользователей в DOMAIN. Регламенты технических осмотров. Профилактические работы в объектах сетевой инфраструктуры. Мониторинг и анализ сети с помощью программных и аппаратных средств Структура системы управления, архитектура системы управления. Управление областями сети: ошибками, конфигурацией, доступом, производительностью, безопасностью. Работа с протоколами SNMP; CMIP; TMN; LNMP; ANMP. Отслеживание работы сети. Работа с сервером, чтение голов, работа над ошибками. Контроль доступа, сохранение целостности данных и журналирование. Удаленное администрирование рабочих станций с сервера Удаленное администрирование сервера с рабочих станций, программы для удаленного доступа. Анализ трафика сети. Работа с кабельными сканерами и тестерами, в т.ч. со встроенными сканерами диагностики и управления. Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных таблиц. Создание плана восстановления сети. Восстановление сети после сбоя. Использование в работе контрольно-измерительной аппаратуры, сервисных плат, комплексов. Разработка функциональных схем элементов автоматизированной системы защиты информации. Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование. Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации. Разработка политик безопасности и внедрение их в операционные системы. Настройка IPSec и VPN. Настройка межсетевых экранов. Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств. Настройка защиты беспроводных сетей с помощью систем шифрования. Архивация и восстановление ключей в Windows Server (PKI). Установка и настройка системы обнаружения атак Snort.		
Всего	**216**	
Консультация	**2**	

Общее количество часов, включая практику: **Всего:** **Теоретического обучения** **Практических (лабораторных) занятий** **Самостоятельной работы** **Консультация**	***668*** ***452*** ***153*** ***153*** ***144*** ***2***	

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)

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация профессионального модуля предполагает наличие лабораторий **эксплуатации объектов сетевой инфраструктуры** и **программно-аппаратной защиты объектов сетевой инфраструктуры, а** также полигона **технического контроля и диагностики сетевой инфраструктуры.**

Лаборатория эксплуатации объектов сетевой инфраструктуры;

Оборудование лаборатории и рабочих мест мастерской:

- Оборудование лаборатории и рабочих мест лаборатории: 12 компьютеров учащегося и 1 компьютер преподавателя;
- Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа, обжимной инструмент, коннекторы RJ-45, тестеры для кабеля);
- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности.

Оборудование и технологическое оснащение рабочих мест:

- Компьютер учащегося (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО – CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР)
- Компьютер преподавателя (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО – CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР).
- Сервер в лаборатории (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; Жесткий диск объемом не менее 1Тб; программное обеспечение:Windows Server 2003 или Windows Server 2008; лицензионные антивирусные программы; лицензионные программы восстановления данных.

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением
- интерактивная доска
- проектор

Лаборатория программно-аппаратной защиты объектов сетевой инфраструктуры:

Оборудование мастерской и рабочих мест мастерской:

- Оборудование лаборатории и рабочих мест лаборатории: 12 компьютеров учащихся и 1 компьютер преподавателя;
- Типовое активное оборудование: сетевые маршрутизаторы, сетевые коммутаторы, сетевые хранилища, сетевые модули и трансиверы, шасси и блоки питания, шлюзы VPN, принт-серверы, IP – камеры, медиа-конвертеры, сетевые адаптеры и карты, сетевые контроллеры, оборудование xDSL, аналоговые модемы, коммутационные панели, беспроводные маршрутизаторы, беспроводные принт-серверы, точки доступа WiFi, WiFi – адаптеры,

Bluetooth – адаптеры, KVM-коммутаторы, KVM-адаптеры, VoIP маршрутизаторы, VoIP-адаптеры;

- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности.

Оборудование и технологическое оснащение рабочих мест:

- Компьютер учащегося (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО – CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР)
- Компьютер преподавателя (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО – CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР)
- Сервер в лаборатории (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; Жесткий диск объемом не менее 1Тб; программное обеспечение:Windows Server 2003 или Windows Server 2008; лицензионные антивирусные программы; лицензионные программы восстановления данных.

Перечень программного обеспечения:

1. Ethereal, разработчик – Gerald Combs (C) 1998-2005, источник – http://www.ethereal.com, версия 0.10.11.
2. InterNetView, разработчик – Evgene Ilchenko, источник – http://www.tsu.ru /~evgene/info/inv, версия 2.0.
3. Netcat, разработчик – Weld Pond <weld@l0pht.com>, источник – http://www. l0pht.com, версия 1.10.
4. Nmap, разработчик – Fyodor (Gordon Lyon), источник – https://nmap.org/, версия 7.60.
5. Snort, разработчик – Martin Roesch & The Snort Team. Copyright 1998–2005 Sourcefire Inc., et al., источник – http://www.snort.org, версия 2.4.3.
6. VipNet Office, разработчик – ОАО Инфотекс, Москва, Россия, источник – http://www.infotecs.ru, версия 2.89 (Windows).
7. VMware Workstation, разработчик – VMware Inc, источник – http://www. vmware.com, версия 4.0.0.
8. WinPCap, источник – http://winpcap.polito.it.
9. AdRem Netcrunch, источник – http://www.adremsoft.com/netcrunch/
10. OpenVAS, источник – http://www.openvas.org/

3. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Самостоятельная работа студентов (СРС) – это планируемая учебная работа, выполняемая по заданию преподавателя под его методическим и научным руководством.

СРС по данной дисциплине включает:

- подготовку к аудиторным занятиям (проработка пройденного учебного материала по конспектам, рекомендованной преподавателем учебной и научной литературе; изучение учебного материала, перенесенного с аудиторных занятий на самостоятельную проработку);
- подготовка к практическим занятиям (решение домашних заданий (задач, упражнений и т.п.));
- выполнение индивидуальных самостоятельных работ и заданий (расчетно-графическая работа, контрольная работа).

Распределение бюджета времени на выполнение индивидуальных СРС представлено в таблице 3.

Таблица 3 – Учебно-методическая (технологическая) карта СРС

Номер раздела и темы дисциплины	Код и наименование индивидуального проекта – задания или вида СРС	Объем часов на СРС	Сроки выпо-ния	Реко-мендуемые УММ	Форма контроля СРС
1	2	3	4	5	6
Раздел 1.	ИЗ № 1 (индивидуальное задание) – расчетно-графическая работа	10	3нед.		Защита РГР, решение примеров
Раздел 3.	ИЗ № 2 – расчетно-графическая работа	10	3 нед.		Защита РГР. Коллоквиум по теории
Раздел 6.	ИЗ № 3, 4 (индивидуальные задания) – расчетно-графическая работа	10	4нед.		
	Подготовка отчетов для защиты	10	3 нед.		
Общие затраты времени студентом по всем видам СРС					
СРС: подготовка к лекционным занятиям			40		
СРС: подготовка к практическим занятиям			40		
СРС: выполнение индивидуальных , РГ и К работ			40		
Подготовка к тестированию и ДЗ			24		
Итого:			144		

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 4 – Учебно-методическое обеспечение профессионального модуля «эксплуатации объектов сетевой инфраструктуры» учебно-методическими материалами

Код и наименование специальности	Учебно-методический материал		Количество экземпляров	
	№№	Наименование	всего	На 1 обучающегося, приведенного к оч. ф
09.02.02 «Компьютерные сети»	**Основная литература**			
	1			
	2	Мищенко, П.В. Маршрутизация в составных сетях : учеб.-метод. пособие / П.В. Мищенко .— Новосибирск : Изд-во НГТУ, 2016 .— 72 с. : ил. https://rucont.ru/efd/586668		
	3	Васин, Н.Н. Технологии пакетной коммутации. Ч. 1. Основы построения сетей пакетной коммутации : метод. указания к лаб. работам / Н.Н. Васин .— Самара : Изд-во ПГУТИ, 2014 .— 24 с. : ил. https://rucont.ru/efd/565017		
	4	Галимов, Р.Р. Программно-аппаратные средства защиты информации : метод. указания / А.А. Рычкова, Оренбургский гос. ун- т, Р.Р. Галимов .— Оренбург : ОГУ, 2015 .— 89 с. : ил. https://rucont.ru/efd/304038		
	5	Основы теории передачи информации : учебное пособие для студентов, обучающихся по специальности "Вычислительные машины, комплексы, системы и сети" / О. С. Литвинская, Н. И. Чернышёв. - Москва : КНОРУС, 2015. - 168 с.		
	6	Сердюк, А. И. Криптография. Разработка приложений для шифрования информации : метод. указания / О. Н. Яркова, А. И. Сердюк .— Оренбург : ГОУ ОГУ, 2012 .— 98 с. : ил. http://api.rucont.ru/api/efd/reader?file=204999		
	Дополнительная литература			
	7	Конфигурирование сетей CISCO. Часть 1 / С.В. Архипов, А.М. Цыденмункуев .— Улан-Удэ : Бурятский государственный университет, 2016 .— 158 с. https://rucont.ru/efd/558891		
	8	Цыбулин, А. М. Лабораторный практикум по дисциплине «Программно-аппаратные средства		

		защиты информации» : учеб.-метод. пособие / В. С. Аткина, М. Ю. Умницын, Волгогр. гос. ун-т, А. М. Цыбулин .— Волгоград : Изд-во ВолГУ, 2012 .— 177 с. : ил. https://rucont.ru/efd/246171		
	9	Маршрутизация и коммутации /Васин Н. http://www.intuit.ru/studies/courses/3646/888/info		
	10	Основы построения сетей пакетной коммутации /Васин Н. http://www.intuit.ru/studies/courses/3645/887/info		
		Насейкина, Л. Ф. Основы проектирования компьютерных сетей : метод. указания / В. К. Тагиров, Оренбургский гос. ун- т, Л. Ф. Насейкина .— Оренбург : ОГУ, 2014 .— 84 с. : ил. https://rucont.ru/efd/293602		
		Технологии разработки и создания компьютерных сетей на базе аппаратуры D-LINK : учеб. пособие / В.В. Баринов, А.В. Благодаров, Е.А. Богданова, А.Н. Пылькин, Д.М. Скуднев .— М. : Горячая линия – Телеком, 2013 .— 217 с. : ил. https://rucont.ru/efd/214212		
		Долозов, Н. Л. Компьютерные сети : учеб.-метод. пособие / Н. Л. Долозов .— Новосибирск : Изд-во НГТУ, 2013 .— 112 с. https://rucont.ru/efd/246624		
		Шелухин, О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учеб. пособие / Д.Ж. Сакалема, А.С. Филинова, О.И. Шелухин .— М. : Горячая линия – Телеком, 2013 .— 221 с. : ил https://rucont.ru/efd/214235		

5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

В таблице 5 представлены общеуниверситетские ресурсы и ресурсы колледжа, которые должны быть использованы для полноценного изучения дисциплины.

Таблица 5 – Сведения об оснащенности образовательного процесса специализированным и лабораторным оборудованием

Используемые специализированные аудитории и лаборатории		
№	Наименование	Оборудование
1	Лекционная аудитория	Интерактивная доска, ноутбук, проектор
2	Учебный кабинет «ЭОСИ»	ПК в количестве 10-15

6. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Таблица 6. Формы и методы контроля результатов обучения.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
В результате освоения дисциплины обучающийся должен: **иметь практический опыт:** – обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя; – удаленного администрирования и восстановления работоспособности сетевой инфраструктуры; – организации бесперебойной работы системы по резервному копированию и восстановлению информации; – поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры; **уметь:** – выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; – использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры; – осуществлять диагностику и поиск неисправностей технических средств; – выполнять действия по устранению неисправностей в части, касающейся полномочий техника; – тестировать кабели и коммуникационные устройства; – выполнять замену расходных материалов и мелкий ремонт периферийного оборудования; – правильно оформлять техническую документацию; – наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных; – устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту; **знать:** – архитектуру и функции систем управления сетями, стандарты систем управления; – задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией; – средства мониторинга и анализа локальных сетей; – классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; – правила эксплуатации технических средств сетевой инфраструктуры; – расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;	Практические занятия Устный ответ у доски Проверка домашних заданий Контрольные работы Тестирование Самостоятельная работа по индивидуальным заданиям Дифференцированный зачет

– методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных; – основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем (ИС), требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.	