

бюджетное профессиональное образовательное учреждение
Вологодской области
«Грязовецкий политехнический техникум»



Фонд оценочных средств

по профессиональному модулю:

ПМ. 03 «ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ»

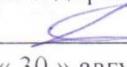
09.02.02 Компьютерные сети

Грязовец
2017 г.

Рассмотрен

цикловой комиссией общепрофессиональных
дисциплин и профессиональных модулей
отделения «Электрификация
и автоматизация сельского хозяйства»

Согласовано

зам. директора по ОМР
 Е. А. Ткаченко
« 30 » августа 2017 г.

Протокол № 1 от « 30 » августа 2017 г.

Председатель комиссии:

 Т. В. Невзорова

1.Общие положения

Фонд оценочных средств (ФОС) предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу профессионального модуля ПМ. 03 Эксплуатация объектов сетевой инфраструктуры. ФОС включает контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме дифференцированного зачета.

ФОС разработаны на основании положений:

ФГОС СПО специальности 09.02.02 Компьютерные сети утвержденного приказом Министерства образования и науки Российской Федерации от 28.07.2014 N 803

основной профессиональной образовательной программы по специальности 09.02.02 Компьютерные сети программы профессионального модуля ПМ. 03 Эксплуатация объектов сетевой инфраструктуры.

2. Перечень основных показателей оценки результатов, элементов практического опыта, знаний и умений, подлежащих текущему контролю и промежуточной аттестации

Код и наименование основных показателей оценки результатов (ОПОР)	Код и наименование элемента практического опыта	Код и наименование элемента умений	Код и наименование элемента знаний
1	2	3	4
ОПОР 3.1.1. Установление, настраивание, эксплуатирование и обслуживание технических и программно-аппаратных средств компьютерных сетей	ПО1. Обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя	У1 - выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств	31 - архитектуру и функции систем управления сетями, стандарты систем управления
ОПОР 3.2.1. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях	ПО4. Поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	У4 - выполнять действия по устранению неисправностей в части, касающейся полномочий техника	33 - средства мониторинга и анализа локальных сетей

			39 - основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем
ОПОР 3.3.1. Осуществление эксплуатации сетевых конфигураций	ПО4. Поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	У5 - тестировать кабели и коммуникационные устройства	35 - правила эксплуатации технических средств сетевой инфраструктуры
			36 - расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры
ОПОР 3.4.1. Разработка схем послеаварийного восстановления работоспособности компьютерной сети, выполнение восстановления и резервное копирование информации	ПО2. Удаленного администрирования и восстановления работоспособности сетевой инфраструктуры	У2 - использовать схемы послеаварийного восстановления работоспособности сети эксплуатировать технические средства сетевой инфраструктуры	37 - методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных
	ПО3. Организации бесперебойной работы системы по резервному копированию и восстановлению информации	У8 - наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных	
ОПОР 3.5.1. Организация инвентаризации технических средств сетевой инфраструктуры, осуществление контроля	ПО1. Обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя	У3 - осуществлять диагностику и поиск неисправностей технических средств	34 - классификацию регламентов, порядок технических осмотров, проверок и профилактических работ

поступившего из ремонта оборудования		У7 - правильно оформлять техническую документацию	
ОПОР 3.6.1. Выполнение замены расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры.	ПО4. Поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры	У3 - осуществлять диагностику и поиск неисправностей технических средств	34 - классификацию регламентов, порядок технических осмотров, проверок и профилактических работ
		У6 - выполнять замену расходных материалов и мелкий ремонт периферийного оборудования	

3. Распределение основных показателей оценки результатов по видам аттестации

Профессиональные компетенции по ФГОС	Основные показатели оценки результатов	Виды аттестации				
		«внутренняя» система оценки			«внешняя» система оценки	
		Текущий контроль	Промежуточная аттестация		Государственная (итоговая) аттестация	
			Теоретический экзамен	Практика		
		учебная		производственная (преддипломная)		
ПК 3.1 Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей	ОПОР 3.1.1. Установление, настраивание, эксплуатирование и обслуживание технических и программно-аппаратных средств компьютерных сетей	+			+	+
ПК 3.2 Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях	ОПОР 3.2.1. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях	+			+	+
ПК 3.3 Эксплуатация сетевых конфигураций	ОПОР 3.3.1. Осуществление эксплуатации сетевых конфигураций	+			+	+
ПК 3.4 Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации	ОПОР 3.4.1. Разработка схемы послеаварийного восстановления работоспособности компьютерной сети, выполнение восстановления и резервное копирование информации	+			+	+
ПК 3.5 Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования.	ОПОР 3.5.1. Организация инвентаризации технических средств сетевой инфраструктуры, осуществление контроля поступившего из ремонта оборудования	+			+	+
ПК 3.6 Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	ОПОР 3.6.1. Выполнение замены расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой	+			+	+

	инфраструктуры.					
--	-----------------	--	--	--	--	--

4.Кодификатор контрольных заданий

Функциональный признак оценочного средства (тип контрольного задания)	Метод/форма контроля	Код контрольного задания
Проектное задание	Учебный проект (курсовый, исследовательский, обучающий, сервисный, социальный творческий, рекламно-презентационный)	1
Реферативное задание	Реферат	2
Расчетная задача	Контрольная работа, индивидуальное домашнее задание, лабораторная работа, практические занятия, письменный экзамен	3
Поисковая задача	Контрольная работа, индивидуальное домашнее задание	4
Аналитическая задача	Контрольная работа, индивидуальное домашнее задание	5
Графическая задача	Контрольная работа, индивидуальное домашнее задание	6
Задача на программирование	Контрольная работа, Индивидуальное домашнее задание	7
Тест, тестовое задание	Тестирование, письменный экзамен	8
Практическое задание	Лабораторная работа, практические занятия, практический экзамен	9
Экзаменационное задание	Письменный/устный экзамен	10
Ролевое задание	Деловая игра	11
Исследовательское задание	Исследовательская работа	12
Доклад, сообщение		13
Задание на ВКР дипломный проект	Выпускная квалификационная работа СПО	14
Задание на ВКР дипломная работа	Выпускная квалификационная работа СПО	15

5. Содержательно - компетентностная матрица оценочных средств текущего контроля (распределение типов и количества контрольных заданий по элементам знаний и умений)

Содержание учебного материала по программе ПМ	Код контрольного задания																		Количество контрольных заданий по типам												
	ПО1	У1	У4	З1	З3	ПО4	У9	З2	З8	З9	ПО4	У5	З5	З6	ПО2	ПО3	У2	У8	З7	ПО1	У3	У7	З4	ПО4	У3	У6	З4	2	3	8	9
Раздел 1. Тема 1.1. Эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей	9			13		9	9		8		9						9		8		9			9		13		2	8	2	
Раздел 1. Тема 1.2. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях	9	9		8		9				9				8	9		13		9		8	9		9			3	8	1		
Раздел 1. Тема 1.3. Эксплуатация сетевых конфигураций		9		8			9		13	9						9	9			9			9	9			1	8	1		
Раздел 1. Тема 1.4 Средства мониторинга и анализа локальных сетей			9			9		8		9		8		9						9			9		8		3	6			
Раздел 1. Тема 1.5 Хранение информации		9			8		9		13		9		8					13		9			9			2	5	2			
Раздел 1. Тема 1.6 Схема после аварийного восстановления				8					8							9	9			9					8		3	3			

<i>Раздел 1. Тема 1.7. Диагностика неисправностей технических средств и сетевой структуры</i>	9	9			13	9		8		9		8		9	9		9	8						3	7	1	
<i>Раздел 2. Тема 2.1. Основные понятия информационной безопасности</i>			9	13					1 3		9				9	8		9	9			9	9		1	7	2
<i>Раздел 2. Тема 2.2. Компьютерные вирусы</i>					9				13		9			9	9			9	13						5	2	
<i>Раздел 2. Тема 2.3. Организация защиты информации в сетях</i>	9		9		8	9	9		8		9	9		9	9		9	9			9	9	9		2	14	
<i>Раздел 3. Тема 3.1.. Организация, принципы построения и функционирования сетей IP-телефонии</i>				8			9		8	8			13		9	9		9	9			9	9		3	7	1
<i>Раздел 3. Тема 3.2. Администрирование сетей IP-телефонии</i>	9	9	9					8		9	9				9			13							1	6	1
<i>Итого:</i>																								24	84	13	

6. Содержательно - компетентностная матрица оценочных средств промежуточной аттестации

Содержание учебного материала по программе ПМ	Код контрольного задания																Количество контрольных заданий по типам																	
	ОПОР 3.1.1.				ОПОР 3.2.1.				ОПОР 3.3.1.				ОПОР 3.4.1.				ОПОР 3.5.1.		ОПОР 3.6.1.															
	ПО1	У1	У4	З1	З3	ПО4	У9	З2	З8	З9	ПО4	У5	З5	З6	ПО2	ПО3	У2	У8	З7	ПО1	У3	У7	З4	ПО4	У3	У6	З4	8	9	13				
Раздел 1. Тема 1.1. Эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей		9			8																													
Раздел 1. Тема 1.2. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях	9				9				8						9																2	3		
Раздел 1. Тема 1.3. Эксплуатация сетевых конфигураций			9			9		8					8			9																2	3	
Раздел 1. Тема 1.4. Средства мониторинга и анализа локальных сетей				8				8		9					9																	2	3	
Раздел 1. Тема 1.5. Хранение информации	9								8			8			8			9			9			9							2	4		

<i>Раздел 1. Тема 1.6 Схема после аварийного восстановления</i>				8					9			9			9			1	3
<i>Раздел 1. Тема 1.7. Диагностика неисправностей технических средств и сетевой структурь</i>					9							9							2
<i>Раздел 2. Тема 2.1. Основные понятия информационной безопасности</i>		9				8		9										1	2
<i>Раздел 2. Тема 2.2. Компьютерные вирусы</i>								8							8			2	
<i>Раздел 2. Тема 2.3. Организация защиты информации в сетях</i>				8						9								1	1
<i>Раздел 3. Тема 3.1.. Организация, принципы построения и функционирования сетей IP- телефонии</i>		9			8							8					8	3	1
<i>Раздел 3. Тема 3.2. Администрирование сетей IP- телефонии</i>				8						9								1	1
<i>Итого:</i>																	20	26	0

7. Содержательно - компетентностная матрица оценочных средств государственной (итоговой) аттестации (распределение типов количества контрольных заданий по ОПОР и ПК)

8. Структура банка контрольных заданий ФОС

Код контрольного задания	Тип контрольного задания	Количество контрольных заданий	Время выполнения контрольного задания, час	Общее время выполнения контрольных заданий, час
2	Реферативное задание			
3	Расчетная задача			
8	Тест, тестовое задание	44	0,5	22
9	Практическое задание	110	1	110
10	Экзаменационное задание			
13	Доклад, сообщение	13	2	26
14	Задание на ВКР дипломный проект	12	8	96
Итого:		179	11,5	254

Оценка освоения теоретического курса профессионального модуля

Основной целью оценки теоретического курса профессионального модуля является оценка умений и знаний.

Оценка теоретического курса профессионального модуля осуществляется с использованием следующих форм и методов контроля: для текущего, промежуточного контроля используется – тестирование, выполнение ЛПЗ и дифференцируемый зачет.

1. Типовые задания для оценки освоения МДК 03.01 Эксплуатация объектов сетевой инфраструктуры:

1. Основное предназначение всех сетевых технологий?

1. обеспечение выхода всех ЛВС в глобальную сеть
2. обеспечение надежных соединений между компьютерами
3. обмен информацией между ЛВС и глобальной сетью
4. связь объектов, находящихся на большом расстоянии друг от друга

2. Что НЕ является каналом передачи данных?

1. витая пара
2. коаксиальный кабель
3. алюминиевая жила
4. оптоволокно

3. Что помогает более гибко настраивать сеть при её расширении?

1. нормативы
2. инструменты
3. приборы
4. стандарты

4. Что относится к активному оборудованию?

1. свитч
2. кабельный тестер
3. патч - корд
4. кримпер

5. Из чего можно построить простую компьютерную сеть?

1. из трех ПК и свитча
2. не менее 10 ПК и маршрутизатора
3. из двух ПК, соединенных прямым кабелем
4. из двух ПК, соединенных кроссоверным кабелем

6. Что понимают под физической инфраструктурой сети?

1. сетевое оборудование, соединенное кабелем

2. топологию со всем сетевым оборудованием и транспортными технологиями
3. ПК с прописанными IP - адресами
4. сетевое оборудование, каналы связи и протоколы передачи данных

7. Основная и наиболее протяженная часть компьютерной сети.

1. сегмент
2. телефонная линия связи
3. структурированная кабельная система
4. патч - панель

8. Процесс прямого или обратного преобразования имен?

1. разрешение имен
2. аутентификация
3. идентификация
4. адресация

9. Логические интерфейсы между программными и аппаратными средствами?

1. идентификация
2. сетевые подключения
3. разрешение имен
4. адресация

10. Правила взаимодействия сетевых компьютеров и других устройств?

1. программные приложения
2. сетевые операционные системы
3. IP - адреса
4. сетевые протоколы

11. Экспертиза различных технических объектов специалистами.

1. технический паспорт
2. техническое задание
3. технический регламент
4. техническое освидетельствование

12. Что понимают под управлением компьютерной сетью?

1. поддержание её в работоспособном состоянии
2. автоматизация процессов контроля и настройки параметров
3. поддержание соответствующего уровня производительности
4. прогнозирование сбоев и перегрузки

13. Что подразумевает под собой создание пользователя?

1. получение IP адреса
2. доступ ко всем ресурсам сервера

3. создание новой учетной записи
 4. создание структуры директорий для хранения документов сайта и создание соответствующей записи в конфигурации сервера
- 14. Что в сети контролирует порты и обращение программ к сетевым интерфейсам?**
1. сетевые экраны
 2. антивирусные программы
 3. протокол TCP/IP
 4. анализатор протоколов
- 15. Какой протокол управления сетью является протоколом взаимодействия между агентами и менеджерами системы управления?**
1. TCP/IP
 2. SNMP
 3. CMIP
 4. TMN
- 16. Что подразумевает под собой создание домена?**
1. создание структуры директорий для хранения документов сайта и создание соответствующей записи в конфигурации сервера
 2. доступ ко всем ресурсам сервера
 3. получение IP адреса
 4. создание новой учетной записи
- 17. Быстро проверить качество работы только что настроенной локальной сети поможет**
1. кабельный тестер
 2. утилита ping
 3. сетевая операционная система
 4. протокол TCP/IP 4версии
- 18. Что относится к процессам управления конфигурациями?**
1. сбор статистики использования устройств
 2. составление отчетности
 3. отслеживание нагрузки сетевых узлов
 4. настройка параметров
- 19. Контроль доступа к сетевым ресурсам, чтобы предотвратить несанкционированный доступ – это ...**
1. управление неисправностями
 2. управление защитой данных
 3. управление учетом сетевых ресурсов
 4. управление операциями
- 20. Альтернативой сетевому адресу является...**
1. IP - адрес
 2. MAC – адрес
 3. идентификатор

4. общий сетевой адрес

21. Что определяет производительность сети?

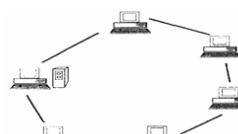
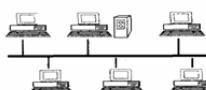
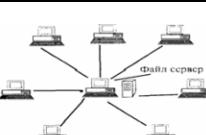
1. мониторинг трафика
2. оперативная работа администратора
3. скорость передачи пакетов
4. скорость обработки пакетов

22. Это свойство сети означает возможность сравнительно легкое добавление отдельных элементов сети, наращивания длины сегментов и замены аппаратуры на более мощную.

23. Как называется процедура проверки кабельной системы?

24. Укажите имя организации в сети WWW.ARZNET.API.REC.RU

25. Поставьте соответствие между топологией сети и ее графическим изображением:

1.«общая шина»	 1.
2.звезда	 2.
3.кольцо	 3.

26. Поставьте соответствие между пассивным оборудованием и его назначением:

1. Розетка	1. коммутационный кабель, соединяющий конечного пользователя с сетью, или использующийся для подключения активного сетевого оборудования.
2.Патч-корд	2.защищают информационный кабель от повреждений, изломов, агрессивного воздействия внешней среды и доступа посторонних.
3.Патч - панели	3.конечная точка, к которой подводится кабель-канал или скрытый за стеной кабель

27. Поставьте соответствие между активным оборудованием и его назначением:

1. Повторители	1. это программно – аппаратные устройства, которые делят общую среду передачи данных на логические сегменты
2. Концентраторы	2. это коммуникационное оборудование (например, компьютер), служащее для объединения разнородных сетей с различными протоколами обмена
3. Коммутаторы	3. это аппаратные устройства, предназначенные для восстановления и усиления сигналов в вычислительных сетях с целью увеличения их длины
4. Мосты	4. это коммуникационное оборудование, которое обеспечивает выбор маршрута передачи данных между несколькими сетями, имеющими различную архитектуру или протоколы
5. Маршрутизаторы	5. это программно – аппаратные устройства, которые обеспечивают соединение нескольких локальных сетей между собой или несколько частей одной и той же сети, работающих с разными протоколами
6. Шлюзы	6. – это аппаратные устройства множественного доступа, которые объединяют в одной точке отдельные физические отрезки кабеля, образуют общую среду передачи данных или физические сегменты сети

28. Расположите шаги алгоритма Настройка домашней локальной сети по порядку выполнения:

1. Включение Брандмауэр Windows.
2. Прописывание сетевых настроек на всех компьютерах/ ноутбуках/ телевизорах сети (этот шаг используется при отсутствии роутера в локальной сети).
3. Проверка имени компьютеров и рабочей группы прописанных в свойствах компьютеров.

4. Проверка работы сети.

29. Разложите провода витой пары по цветам в соответствии со стандартом Т568В.

1. бело - коричневый

2. коричневый
3. бело - зеленый
4. бело – оранжевый
5. синий
6. оранжевый
7. бело – синий
8. зеленый

30. Расположите шаги алгоритма Управления отказами в работе сети по порядку выполнения:

1. Изолирование проблемы
2. Запись информации об обнаружении и исправлении проблемы
3. Определение симптомов проблемы
4. Обнаружение и устранение во всех важных подсистемах
5. Устранение проблемы

Критерии оценки:

Тестовые оценки необходимо соотнести с общепринятой пятибалльной системой:

- ✓ оценка «5» (отлично) выставляется студентам за верные ответы, которые составляют 90 % и более от общего количества вопросов;
- ✓ оценка «4» (хорошо) соответствует результатам тестирования, которые содержат от 80 % до 90 % правильных ответов;
- ✓ оценка «3» (удовлетворительно) от 60 % до 79 % правильных ответов;
- ✓ оценка «2» (неудовлетворительно) соответствует результатам тестирования, содержащие менее 60 % правильных ответов

Вопросы к дифференцированному зачету по междисциплинарному курсу

Тема 1.1. Эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей

1. Дайте определения терминам «телекоммуникация», «сигнал». Опишите работу системы телекоммуникации (СТК) по структурной схеме.
2. Назовите назначение и составные части первичной и вторичной сетей сети страны РФ.
3. Опишите структуру Федеральной сети Российской Федерации, назначение ее элементов.
4. Перечислите комплекс работ по развёртыванию физической инфраструктуры сетей.
5. Назовите этапы развёртывания сетевой инфраструктуры предприятия.

6. Перечислите групповые роли и задачи персонала на этапе разработки новой компьютерной системы.
7. Опишите действия, которые необходимо выполнить до развёртывания целевой операционной системы на целевом компьютере
8. Перечислите мероприятия, проводимые в процессе технической эксплуатации (ТЭ) ЛВС и рекомендуемые методы технического обслуживания объектов ТЭ:
9. Перечислите виды отказов объектов технической эксплуатации и дайте их краткую характеристику
10. Назовите виды управляемого технического обслуживания сети. Рассмотрите особенности непрерывного эксплуатационного контроля.
11. Назовите виды управляемого технического обслуживания сети. Перечислите заключения о работоспособности объекта, выносимые по результатам оперативно-технического контроля состояния сети.
12. Дайте определения терминам «Маршрутизатор», «Маршрутизация». Перечислите основные действия маршрутизатора, выполняемые им для реализации своих функций.
13. Перечислите группы методов доступа компьютеров к сети. Рассмотрите подробней методы случайногo доступа к сети.
14. Перечислите группы методов доступа компьютеров к сети. Рассмотрите подробней методы детерминированного доступа к сети.
15. Опишите методы коммутации в телекоммуникационных сетях (ТКС).
16. Перечислите основные технологии масштабирования. Опишите технологию нивелирования времени ожидания связи
17. Перечислите основные технологии масштабирования. Опишите технологию распределения.
18. Перечислите основные технологии масштабирования. Опишите технологию репликации компонентов распределённой системы.
19. Объясните порядок работ при проектировании ЛВС, перечислите руководящие документы, регламентирующие данный вид работ, состав проектной документации ЛВС (стадия «П»).
- 20 Перечислите состав и краткое содержание рабочей документации при проектировании ЛВС (стадия «Р»), их соответствие различным этапам работ.

Тема 1.2. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях.

1. Дайте определение термину «техническое обслуживание (ТО)». Перечислите основные методы ТО. Опишите статистический метод ТО сетевых объектов.
2. Дайте определение термину «техническое обслуживание (ТО)». Перечислите основные методы ТО. Опишите профилактический метод ТО оборудования.

3. Дайте определение термину «техническое обслуживание (ТО)». Перечислите основные методы ТО. Опишите восстановительный метод ТО сетевых объектов.

4. Опишите способы и системы переключения на резерв для кабельных, волноводных и радиорелейных линий связи, а также виды переключений, применяемые на практике.

5. Опишите способы увеличения надёжности кабельной системы и сети

6. Перечислите способы резервирования систем оптической связи. Опишите способ линейного резервирования.

7. Перечислите способы резервирования систем оптической связи. Опишите способ системного резервирования.

8. Назовите мероприятия, проводимые при техническом обслуживании (ТО) технических компонентов ЛВС, виды ТО. Перечислите применяемое оборудование и виды работ при проведении индивидуального ТО.

9. Назовите мероприятия, проводимые при техническом обслуживании (ТО) технических компонентов ЛВС, виды ТО. Перечислите применяемое оборудование и виды работ при проведении группового ТО.

10. Укажите порядок проведения централизованного технического обслуживания (ТО), перечень работ, проводимых при этом виде ТО, а также операции, которым подвергается сетевое оборудование в процессе эксплуатации.

11. Перечислите группы мероприятий по техническому обслуживанию (ТО) технических компонентов ЛВС, мероприятия, проводимые при ТО существующей ЛВС.

12. Перечислите основные этапы при проведении аудита ЛВС, перечень работ по техническому обслуживанию ЛВС.

13. Опишите принципы построения структурированной кабельной системы (СКС).

14. Опишите состав и назначение подсистем структурированной кабельной системы.

15. Обоснуйте необходимость централизованной системы контроля и управления крупной корпоративной сетью.

Тема 3. Эксплуатация сетевых конфигураций

1. Перечислите основные группы задач систем управления сетями. Опишите задачи, выполняемые функциональной группой управления конфигурацией сети

2. Перечислите основные группы задач систем управления сетями. Опишите задачи, выполняемые функциональной группой обработки ошибок.

3. Перечислите основные группы задач систем управления сетями. Опишите задачи, выполняемые функциональной группой анализа производительности и надёжности.

4. Перечислите основные группы задач систем управления сетями. Опишите задачи, выполняемые функциональной группой управления безопасностью.

5. Перечислите основные группы задач систем управления сетями. Опишите задачи, выполняемые функциональной группой учёта работы сети.
6. Опишите функции, выполняемые системой управления компьютерами и их системным и прикладным ПО (System Management System).
7. Перечислите функциональные группы системы управления сетями IBM, ориентированных на пользователя. Опишите функцию управления конфигурацией
8. Перечислите функциональные группы системы управления сетями IBM, ориентированных на пользователя. Опишите функцию управления производительностью и учётом использования ресурсов
9. Перечислите функциональные группы системы управления сетями IBM, ориентированных на пользователя. Опишите функцию управления проблемами
10. Перечислите функциональные группы системы управления сетями IBM, ориентированных на пользователя. Опишите функцию управления операциями
11. Перечислите функциональные группы системы управления сетями IBM, ориентированных на пользователя. Опишите функцию управления изменениями
12. Опишите модель стандарта Telecommunication Management Network (TMN)
13. Перечислите задачи по управлению компьютерными сетями. Опишите протоколы, разработанные для управления ЛВС.
14. Укажите различия между протоколами для управления сетями SNMP и CMIP.
15. Укажите меры безопасности, применяемые при использовании SNMP для мониторинга сети.
16. Назовите принципы стека протоколов TNM.
17. Опишите стандартное решение для агрегирования портов, реализованное в протоколе LACP (Link Aggregation Control Protocol).
18. Дайте характеристику методам, позволяющим уменьшить риск полной утраты работоспособности системы.
19. Перечислите основные параметры, влияющие на эффективное управление производительностью сети. Назовите мероприятия, которые включает в себя управление производительностью.
20. Сформулируйте задачи тестирования и сбора статистики использования устройств сети. Опишите функцию SNMP-менеджера «Определение порога уведомления».
21. Сформулируйте задачи управления безопасностью сети. Перечислите уровни, на которых осуществляется обеспечение безопасности данных. Приведите классификацию инструментов защиты по типу механизма слежения.

Тема 1.4 Средства мониторинга и анализа локальных сетей

1. Перечислите этапы контроля функционирования ЛВС. Опишите группы средств мониторинга и анализа сети.
2. Перечислите задачи, решаемые анализаторами сетевых протоколов. Опишите принцип его работы и состав.
3. Проанализируйте общие свойства анализаторов протоколов.
4. Перечислите виды анализаторов протоколов. Опишите принцип работы программных анализаторов протоколов.
5. Назовите особенности применения программных анализаторов протоколов при использовании в сети коммутаторов.
6. Перечислите виды анализаторов протоколов. Опишите принцип работы аппаратных анализаторов протоколов.
7. Сделайте вывод о необходимости применения экспертных систем для диагностики неисправностей на узлах ЛВС. Перечислите подсистемы средств мониторинга и анализа сетей, используемые для реализации экспертных систем.
8. Дайте характеристику экспертной системе для диагностики неисправностей на узлах ЛВС как системе искусственного интеллекта. Перечислите категории диагностической информации, предоставляемой системой экспертного анализа администратору сети.
9. Опишите задачи, выполняемые типовой экспертной системой (ЭС) диагностики причин аномальной работы сетей. Перечислите ограничения простейших ЭС. Приведите классификацию ЭС.
10. Изложите по структурной схеме принцип работы экспертной системы (ЭС) анализа причин аномальной работы для решения сложных задач глобального поиска наилучшего решения среди множества решений. Опишите процесс рассуждения ЭС.
11. Опишите стандартный интернет-протокол для управления устройствами в IP-сетях SNMP (Simple Network Management Protocol). Объясните схему взаимодействия Менеджер-SNMP-Агент.
12. Сформулируйте назначение протокола удалённого мониторинга RMON. Опишите виды и назначение зондов RMON.
13. Сформулируйте особенности мониторинга коммутируемых сетей

Тема 1.5 Хранение информации

1. Изложите сущность резервного копирования. Назовите проводимые мероприятия при подготовке к восстановлению данных, меры, принимаемые для снижения времени изготовления копии:
2. Опишите правила, которые необходимо соблюдать при организации и (или) оптимизации существующей системы резервного копирования.
3. Перечислите категории данных, подлежащих резервированию.
4. Опишите применяемые типы резервного копирования и алгоритм создания резервных копий с их помощью.
5. Перечислите какие носители используются на практике в качестве резервных носителей. Дайте их краткую характеристику.
6. Перечислите виды архитектур хранения данных, используемых в

настоящее. Опишите технологию Direct Attached Storage (DAS), ее достоинства и недостатки.

7. Перечислите виды архитектур хранения данных, используемых в настоящее. Опишите технологию Network Attached Storage (NAS), ее достоинства и недостатки.

8. Перечислите виды архитектур хранения данных, используемых в настоящее. Опишите технологию Storage Area Network (SAN), ее достоинства и недостатки

9. Назовите назначение и принципы построения хранилищ данных (ХД). Перечислите основные требования к ХД. Укажите отличия ХД от обычной реляционной базы данных.

10. Перечислите основные компоненты хранилищ данных (ХД) и их назначение. Объясните требования, к СУБД для работы с хранилищами данных.

11. Опишите технологию комплексного многомерного анализа данных OLAP (OnLine Analytical Processing). Обоснуйте основные требования, предъявляемые к программным продуктам, реализующим OLAP-технологию обработки данных в хранилищах данных.

12. Перечислите Проблемы, свойственные централизованной архитектуре баз данных. Назовите основные достоинства децентрализованного хранения данных.

13. Опишите принципы построения и функционирования распределенных баз данных.

Тема 1.6 Схема после аварийного восстановления

1. Перечислите задачи, предусмотренные Планом восстановления функционирования системы.

2. Опишите мероприятия по выполнению Плана на разных этапах.

3. Опишите допущения и посылки, применяемые при разработке Плана восстановления функционирования системы.

4. Изложите структуру проекта планирования восстановления данных. Опишите группы задач, выполняемых при восстановлении данных.

5. Сформулируйте задачи, выполняемые при проведении мероприятий по восстановлению данных после сбоя.

Тема 1.7. Диагностика неисправностей технических средств и сетевой структуры

1. Назовите цели и задачи диагностики сети. Укажите отличия между упреждающей и реактивной диагностикой. Перечислите задачи, для решения которых применяется тестирование сети.

2. Опишите принципы, лежащие в основе методов разработки тестовых и диагностических программ локализации неисправностей сети.

3. Назовите цели, для которых применяется нагружочное тестирование

сети. Перечислите общие принципы локализации дефектов при проведении нагружочного тестирования.

4. Укажите типовую последовательность выполнения нагрузочных тестов. Опишите цель проведения и режимы проверки при проведении теста FTest by steps в режиме калибровки с нагрузкой только на сеть.

5. Укажите типовую последовательность выполнения нагрузочных тестов. Опишите цель проведения и режимы проверки при проведении теста FTest all stations с нагрузкой только на сеть.

6. Укажите типовую последовательность выполнения нагрузочных тестов. Опишите цель проведения и режимы проверки при проведении теста FTest all stations с нагрузкой на сеть и сервер.

7. Укажите типовую последовательность выполнения нагрузочных тестов. Опишите цель проведения и режимы проверки при проведении теста FTest by steps (нормальный режим) с нагрузкой только на сеть.

8. Дайте характеристику групп программных средств диагностики компьютерной сети.

9. Перечислите стандарты, используемые при проектирования и обслуживания СКС. Сравните их между собой.

11. Перечислите основные параметры, измеряемые при проведении тестирования каналов и линий СКС. Дайте их краткую характеристику.

12. Опишите виды тестирования СКС в соответствии с международным стандартом. Перечислите категории измеряемых параметров.

13. Изложите основные рекомендации по тестированию СКС.

14. Опишите особенности тестирования оптоволоконных сетей.

15. Перечислите группы оборудование для проверки кабельных систем.

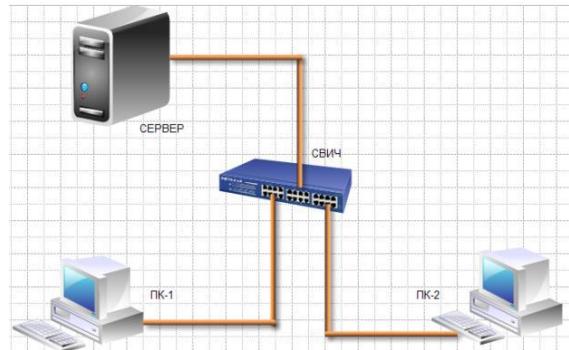
Дайте их краткую характеристику.

16. Перечислите группы оборудование для проверки оптоволоконных СКС. Дайте их краткую характеристику.

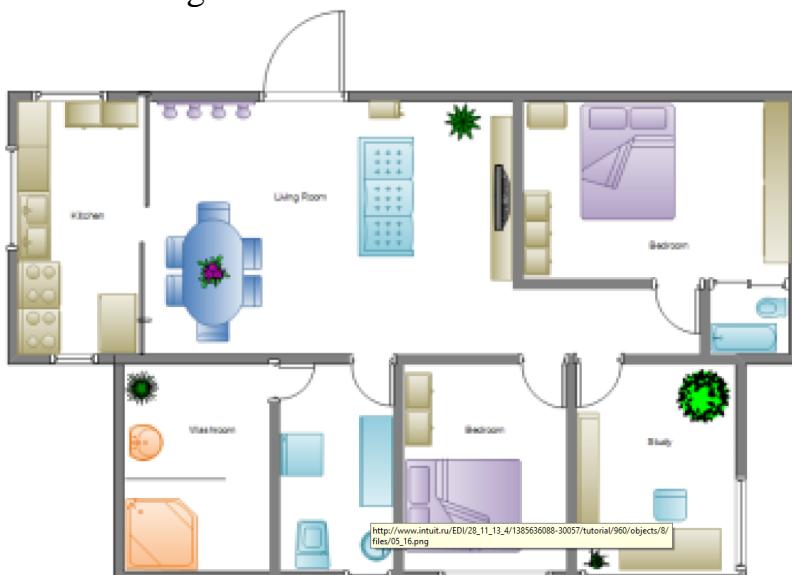
Перечень практических вопросов:

- 1 Создать пользователя USER1 в domain при помощи оснастки «Active Directory – пользователи и компьютеры»
- 2 Создать пользователя USER1 в domain на основании шаблонов.
- 3 Создать пользователей средствами командной строки
- 4 Создать пароль для входа пользователю USER1 в domain
- 5 Создать группы BUH1 и BUH2 в domain при помощи оснастки «Active Directory – пользователи и компьютеры»
- 6 Создать группы BUH1 и BUH2 средствами командной строки
- 7 Создать группы BUH1 и BUH2 и распределить пользователей USER1 и USER12 по группам в domain соответственно.
- 8 Выполнить установку WinRoute
- 9 Выполнить базовую настройку политики трафика в WinRoute
- 10 Выполнить настройку DHCP-сервера в WinRoute
- 11 Выполнить настройку DNS Форвардера в WinRoute

- 12 Выполнить установку CommView Remote Agent и продемонстрировать возможности наблюдения трафика сети.
- 13 Построить схему сети с использованием программы 10-Strike LANState
- 14 Построить диаграмму сети с использованием программы EDraw Network Diagrammer



- 15 Построить диаграмму сети с использованием программы EDraw Network Diagrammer



- 16 Построить диаграмму сети с использованием программы EDraw Network Diagramme,



- 17 Выполнить сканирование локальной сети с программой LanSurfer по заданным параметрам

- Создайте профиль для сканирования Моё сканирование
 - Укажите диапазон адресов от 192.168.3.1 до 192.168.3.254
 - Просканируйте сеть
 - Используя возможности программы найдите файл MyTestXSetup.exe
 - Перейдите в папку содержащий данный файл.
- 18 Используя оснастку Event Viewer, продемонстрируйте возможности работы с системными журналами.
- 19 Выполните установку сетевого монитора
- 20 Запишите данные средствами сетевого монитора
- 21 Сохраните кадры в текстовый файл средствами утилиты Netsh.
- 22 Выполните трассировку сети средствами утилиты Netsh
- 23 Продемонстрируйте устранение неполадок с использованием Network Diagnostics Framework
- 24 Продемонстрируйте устранение неполадок с помощью Ping
- 25 Продемонстрируйте устранение неполадок с помощью PathPing
- 26 Настройте сетевую карту, имя компьютера, рабочую группу по заданным параметрам
- 27 Настройте сетевой интерфейс для введения компьютера в domain.

2. Типовые задания для оценки освоения МДК 03.02 Безопасность функционирования информационных систем:

Задание № 1. Выберите один из нескольких вариантов ответа:

1. Информация это -

- 1 сведения, поступающие от СМИ
- 2 только документированные сведения о лицах, предметах, фактах, событиях
- 3 сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
- 4 только сведения, содержащиеся в электронных базах данных

2. Информация

- 1 не исчезает при потреблении
- 2 становится доступной, если она содержится на материальном носителе
- 3 подвергается только "моральному износу"
- 4 характеризуется всеми перечисленными свойствами

3. Какими официальными документами информация отнесена к объектам гражданских прав?

- 1 УК РФ
- 2 Законом РФ "О праве на информацию"
- 3 ГК и законом РФ "Об информации, информатизации и защите информации"

4 Конституцией РФ

4. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется

- 1 достоверной
- 2 конфиденциальной
- 3 документированной
- 4 коммерческой тайной

5. Формы защиты интеллектуальной собственности -

- 1 авторское, патентное право и коммерческая тайна
- 2 интеллектуальное право и смежные права
- 3 коммерческая и государственная тайна
- 4 гражданское и административное право

6. По принадлежности информационные ресурсы подразделяются на

- 1 государственные, коммерческие и личные
- 2 государственные, не государственные и информацию о гражданах
- 3 информацию юридических и физических лиц
- 4 официальные, гражданские и коммерческие

7. К негосударственным относятся информационные ресурсы

- 1 созданные, приобретенные за счет негосударственных учреждений и организаций
- 2 созданные, приобретенные за счет негосударственных предприятий и физических лиц
- 3 полученные в результате дарения юридическими или физическими лицами
- 4 указанные в п.1-3

8. По доступности информация классифицируется на

- 1 открытую информацию и государственную тайну
- 2 конфиденциальную информацию и информацию свободного доступа
- 3 информацию с ограниченным доступом и общедоступную информацию
- 4 виды информации, указанные в остальных пунктах

9. К конфиденциальной информации относятся документы, содержащие

- 1 государственную тайну
- 2 законодательные акты
- 3 "ноу-хай"
- 4 сведения о золотом запасе страны

10. Запрещено относить к информации ограниченного доступа

- 1 информацию о чрезвычайных ситуациях
- 2 информацию о деятельности органов государственной власти
- 3 документы открытых архивов и библиотек
- 4 все, перечисленное в остальных пунктах

11. Какие методы обеспечения информационной безопасности Российской Федерации направлены на создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение,

уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи?

- 1 правовые
- 2 организационно-технические
- 3 экономические
- 4 стратегические

12. Что использует системы защиты информации SecretDisk для хранения паролей?

- 1 накопители на магнитных дисках
- 2 оперативную память компьютера
- 3 электронные ключи
- 4 бумажные носители

13. С какой целью используется теория информации при рассмотрении каналов передачи информационных потоков?

- 1 для повышения эффективности работы каналов связи
- 2 для анализа качества передаваемой информации
- 3 для вычисления количества информации в потоке и пропускной способности канала
- 4 для шифровки передаваемых сообщений

14. Какие преобразования шифра выполняются при операции рассеивания?

- 1 сжатие шифра
- 2 передача текста небольшими частями
- 3 наложение ложных сообщений
- 4 изменение любого знака открытого текста или ключа

15. Сколько типов архитектуры используется при создании системы сертификации в инфраструктуре с открытыми ключами?

- 1 один
- 2 два
- 3 три
- 4 четыре

16. Какой уровень контроля достаточен для ПО, используемого при защите информации с грифом «ОВ»?

- 1 первый
- 2 второй
- 3 третий
- 4 четвертый

17. С какой целью выполняется шифрование кода программ?

- 1 для противодействия дизассемблированию
- 2 для ускорения работы программ
- 3 в целях повышения надежности программного обеспечения
- 4 для упрощения работы пользователей

18. Какая система обеспечивает защиту информации?

- 1 система разграничения доступа субъектов к объектам
- 2 система кодирования информации

3 система управления потоками данных

4 система идентификации

19. Сколько существует классов, на которые подразделяются носители информации на предприятии?

1 два

2 три

3 пять

20. В чем заключается сущность приема "Троянский конь"?

1 это тайное введение в чужую программу команд, которые позволяют ей осуществлять новые, не планировавшиеся владельцем функции, но одновременно сохранять и прежнюю работоспособность

2 это тайное введение в чужую программу команд, которые позволяют ей осуществлять новые, не планировавшиеся владельцем функции

3 это тайное проникновение в чужую программу

21. RAID-массив это

1 набор жестких дисков, подключенных особым образом

2 антивирусная программа

3 вид хакерской утилиты

4 база защищенных данных

22. Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

1 загрузочный вирус

2 макровирус

3 файловый вирус

4 сетевой червь

23. В каких основных форматах существует симметричный алгоритм?

1 блока и строки

2 потока и блока

3 потока и данных

4 данных и блока

24. Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:

1 шифр функциональных преобразований

2 шифр замен

3 шифр перестановок

25. Возможно ли, вычислить закрытый ключ асимметричного алгоритма, зная открытый?

1 нет

2 да

3 в редких случаях

26. Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им массива открытых данных размера n используется в анализе:

- 1 на основе произвольно выбранного шифротекста**
- 2 на основе произвольно выбранного открытого текста**
- 3 правильного ответа нет**

Задание № 2. Выберите несколько вариантов ответа:

27. Отметьте составные части современного антивируса

- 1 модем**
- 2 принтер**
- 3 сканер**
- 4 межсетевой экран**
- 5 монитор**

28. К вредоносным программам относятся:

- 1 потенциально опасные программы**
- 2 вирусы, черви, трояны**
- 3 шпионские и рекламные программы**
- 4 вирусы, программы-шутки, антивирусное программное обеспечение**
- 5 межсетевой экран, брандмауэр**

29. К биометрической системе защиты относятся:

- 1 защита паролем**
- 2 физическая защита данных**
- 3 антивирусная защита**
- 4 идентификация по радужной оболочке глаз**
- 5 идентификация по отпечаткам пальцев**

30. Компьютерные вирусы – это:

- 1) Вредоносные программы, наносящие вред данным.**
- 2) Программы, уничтожающие данные на жестком диске**
- 3) Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.**
- 4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера**
- 5) Это скрипты, помещенные на зараженных интернет-страницах**

Задание № 3. Укажите соответствие для всех 6 вариантов ответа

31. Сопоставьте названия программ и изображений.



1)

a) Antivir



2)

b) DrWeb



3)

c) Nod 32



4)

г) Antivirus Kaspersky



5)

д) Avast



6)

е) AntivirusPanda

Задание № 4. Укажите истинность или ложность вариантов ответа, поставив «да» или «нет»

32. Выразите свое согласие или несогласие.

- ___ Почтовый червь активируется в тот момент, когда к вам поступает электронная почта.
- ___ Если компьютер не подключен к сети Интернет, в него не проникнут вирусы.
- ___ Файловые вирусы заражают файлы с расширениями *.doc, *.ppt, *.xls.
- ___ Чтобы защитить компьютер недостаточно только установить антивирусную программу.
- ___ На Web-страницах могут находиться сетевые черви.

Задание № 5. Запишите ответ

33. Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию.

Ответ: _____

34. Процесс преобразования информации, хранящейся в файле к виду, при котором уменьшается избыточность в ее представлении и соответственно требуется меньший объем памяти для ее хранения.

Ответ: _____

Задание № 6. Укажите порядок следования всех 3 вариантов ответа

35. Укажите порядок действий при наличии признаков заражения компьютера.

- ___ Сохранить результаты работы на внешнем носителе.
- ___ Запустить антивирусную программу.
- ___ Отключиться от глобальной или локальной сети.

Критерии оценки:

Тестовые оценки необходимо соотнести с общепринятой пятибалльной системой:

- ✓ оценка «5» (отлично) выставляется студентам за верные ответы, которые составляют 90 % и более от общего количества вопросов;
- ✓ оценка «4» (хорошо) соответствует результатам тестирования, которые содержат от 80 % до 90 % правильных ответов;
- ✓ оценка «3» (удовлетворительно) от 60 % до 79 % правильных ответов;
- ✓ оценка «2» (неудовлетворительно) соответствует результатам тестирования, содержащие менее 60 % правильных ответов

Вопросы к дифференцированному зачету по междисциплинарному курсу

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
11. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
12. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем

по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

13. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.

14. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).

15. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.

16. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.

17. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.

18. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).

19. Биометрические средства идентификации и аутентификации пользователей.

20. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.

21. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.

22. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.

23. Законодательный уровень применения цифровой подписи.

24. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.

25. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

26. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

27. Средства обеспечения информационной безопасности в ОС Windows'2000. Разграничение доступа к данным. Групповая политика.

28. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows NT/2000/XP. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.

29. Применение средств Windows 2000/XP для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
30. Разграничение доступа к данным в ОС семейства UNIX.
31. Пользователи и группы в ОС UNIX.
32. Пользователи и группы в ОС Windows'2000.
33. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
34. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
35. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
36. Распределенные информационные системы. Удаленные атаки на информационную систему.
37. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
38. Физические средства обеспечения информационной безопасности.
39. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
40. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
41. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
42. Виртуальные частные сети, их функции и назначение.

Практические задания

1. Анализ бизнес-требований к информационной безопасности
2. Разработка концептуального плана защиты.
3. Анализ технических ограничений плана защиты
4. Применение сертификатов для аутентификации и авторизации
5. Проектирование иерархии ЦС.
6. Проектирование административных ролей ЦС
7. Проектирование политики подачи заявок на сертификаты.
8. Проектирование размещения CRL и интервала публикации.
9. Проектирование защиты границ сети.
10. Защита DNS. Проектирование политики IPSec.

3. Типовые задания для оценки освоения МДК 03.03 Эксплуатация систем IP-телефонии:

Вопросы к дифференцированному зачету по междисциплинарному курсу

1. Как работает схема IP-телефонии «компьютер-телефон»?
2. Какое терминальное оборудование используется в схеме связи «компьютер-компьютер»?
3. Как АЦП и ЦАП влияют на связь в процессе разговора между абонентами?
4. Для чего предназначен H.323 терминал?
5. Что такое ТФОП?
6. Что определяет формат E.164?
7. Какие услуги связи организуются при подключении абонентом IP-телефонии?
8. Для чего предназначен шлюз?
9. Что такое VoIP?
10. Какую функцию выполняет протокол H.245?
11. Для чего предназначен протокол SIP?
12. По какой схеме работает протокол SIP?
13. С помощью какого транспортного протокола переносятся сигнальные сообщения SIP?
14. Какие команды запросов использует SIP?
15. Какие команды ответов использует SIP?
16. Для чего предназначен сервер переадресации в схеме построения SIP сети?
17. Какие услуги связи организуются при подключении абонентом IP-телефонии?
18. Что представляет собой команда INVITE?
19. Какой сигнальный порт используется для обмена служебными сообщениями SIP?
20. Чем протокол SIP отличается от протокола H.323?
21. Какие существуют процедуры обработки речи в IP-телефонии?
22. Как происходит обработка речи в соответствии с кодеком PCM?
23. Как происходит обработка речи в соответствии с кодеком CELP?
24. От каких параметров зависит полоса пропускания в IP-телефонии?
25. Назначение конфигурационного файла sip.conf.
26. Какие типы peer можно задавать в sip.conf, их отличия.
27. Назначение конфигурационного файла extensions.conf.
28. Основные настройки UA при подключении к серверу IP телефонии.
29. Как определить зарегистрирован ли клиент на сервере?
30. В чем причина отсутствия звука при соединении абонентов?

31. Как вызвать клиентскую консоль asterisk, ее назначение и использование.
32. Основные функции клиентской консоли asterisk.
33. Отличия настройки конференции с паролем и без.
34. Возможности кластеризации серверов asterisk.
35. Какой объем составляют заголовки в общей полосе пропускания IP-канала?

Бюджетное профессиональное образовательное учреждение
Вологодской области
«Грязовецкий политехнический техникум»

**Вопросы и практические задания для проведения
квалификационного экзамена
По модулю ПМ.03 Эксплуатация объектов сетевой
инфраструктуры**

основной профессиональной образовательной программы
по специальности СПО
09.02.02 Компьютерные сети
(базовой подготовки)

Теоретические вопросы:

1. Перечислите функции маршрутизатора.
2. Дайте определение информационной безопасности в широком смысле.
3. Перечислите виды технических осмотров.
4. Перечислите основные действия по защите информации при эксплуатации вычислительных (компьютерных) систем.
5. Опишите пользовательский интерфейс программы Ethereal. Фильтр отображения пакетов. Поиск кадров
6. Раскройте сущность трёх технологий масштабируемости.
7. Перечислите основные этапы изменения уровня безопасности.
8. Опишите пользовательский интерфейс программы Ethereal. Поиск кадров
9. Рассказать о методах технического обслуживания.
10. Классифицируйте угрозы ИБ по составу и последствиям.
11. Опишите программу Ethereal. Выделение ключевых кадров. Сохранение данных захвата.
12. Перечислите способы резервирования кабельных систем.
13. Классифицируйте угрозы для ИС.
14. Опишите процесс создания безопасной зоны Acronis.
15. Объясните чем обусловлена надёжность ЛВС?
16. Перечислите источники угроз ИБ.
17. Опишите процесс настройки DHCP сервера.
18. Проанализируйте протоколы Ethernet и ARP
19. Перечислите способы переключения на резерв.
20. Классифицируйте угрозы ИБ по типу реализации.
21. Опишите процесс настройки брандмауэра.
22. Проанализируйте протокол ICMP.
23. Перечислите типы резервного копирования.
24. Дайте определение информационной безопасности в узком смысле.
25. Проанализируйте протокол IP.
26. Опишите как осуществляется управление отказами в сети?
27. Классифицируйте угрозы ИБ по характеру возникновения.
28. Проанализируйте протокол TCP
29. Перечислите каковы цели профилактических проверок ОСИС?
30. Дайте определение безопасности данных
31. Объясните принцип анализа рисков проверки политики информационной безопасности предприятия.
32. Дайте определение технического обслуживания.
33. Перечислите основные функции межсетевого экрана.
34. Распишите алгоритм развёртывания служб Active Directory.
35. Перечислите этапы сетевой атаки. Исследование сетевой топологии.
36. В чём сущность восстановительного метода ТО сетей?
37. Классифицируйте угрозы для ЭИС.

- 38.Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы
- 39.Объясните в чём сущность восстановительного метода ТО сетей?
- 40.Перечислите основные подходы к защите сети
- 41.Объясните как осуществляется реализации атак. Выявление атаки на протокол SMB.
- 42.Расскажите о централизованной системе управления сетью.
- 43.Классифицируйте угрозы ИБ.
- 44.Объясните алгоритм настройки VPN.
- 45.Опишите стандарт криптографической защиты AES (Advanced Encryption Standart).
- 46.Перечислите виды телекоммуникационных сетей.
- 47.Дайте определение шифрования данных.
- 48.Объясните алгоритм настройки прокси сервера.
- 49.Опишите отечественный стандарт хэш-функции и цифровой подписи.
- 50.Перечислите какие виды контроля включает управление ТО?
- 51.Перечислите угрозы, связанные с преднамеренными ошибками.
- 52.Опишите алгоритм действий при тестировании кабельных систем.
- 53.Перечислите компоненты межсетевого экрана. Пример реализации политики МЭ.
- 54.Перечислите какие системы называются открытыми?
- 55.Дайте определение биометрических систем.
- 56.Объясните, что такое IP-сеть?
- 57.Классифицируйте угроз по месту возникновения, объекту воздействия, причине возникновения.
- 58.Объясните применение МЭ на основе фильтрующего маршрутизатора.
- 59.Расскажите об архитектуре систем управления сетями.
- 60.Перечислите основные действия по управлению доступом.
- 61.Объясните применение МЭ на основе экранирующего узла
- 62.Опишите схему взаимодействия Агент-Менеджер.
- 63.Перечислите последствия несанкционированного манипулирования информацией.
- 64.Объясните применение технологии трансляции сетевых адресов. Задачи, решаемые VPN.
- 65.Перечислите какую информацию предоставляет администратору сети ЭС?
- 66.Классифицируйте функции защиты управления доступом.
- 67.Объясните принцип туннелирования в VPN.
- 68.Объясните в чём состоит задача сбора статистики использования устройств сети?
- 69.Классифицируйте угрозы ИБ по характеру возникновения.
- 70.Опишите процесс настройки обратной зоны DNS сервера.
- 71.Объясните принцип организации VPN средствами протокола PPTP.
- 72.Классифицируйте средства мониторинга сети?
- 73.Классифицируйте угрозы для ЭИС.

74. Опишите процесс настройки маршрутизатора.
75. Объясните принцип организации VPN средствами СЗИ VipNet.
76. Дайте определение понятий «диагностика» и «тестирование сети».
77. Перечислите основные подходы к защите сети
78. Опишите процесс настройки беспроводной сети.
79. Объясните принцип организации VPN средствами СЗИ StrongNet.
80. Изложите основные принципы локализации неисправностей сети.
81. Дайте определение биометрических систем.
82. Объясните с помощью командной строки получить подробные сведения обо всех сетевых интерфейсах ПК.
83. Объясните принцип организации VPN средствами протокола SSL в Windows Server
84. Для каких целей проводится входное и нагружочное тестирование сети?
85. Перечислите последствия несанкционированного манипулирования информацией.
86. Проверить реальную скорость интернета.
87. Объясните принцип организации сигнатурного анализа и обнаружения аномалий
88. Объясните в чём состоит принцип локализации неисправностей «сверху вниз»?
89. Классифицируйте угрозы ИБ по составу и последствиям.
90. Объясните алгоритм действий при потере соединения с интернетом.
91. Объясните принцип организации обнаружения аномалий в реальном времени и отложенный анализ
92. Перечислите какие типы нагрузочных тестов вам известны?
93. Перечислите основные этапы изменения уровня безопасности.
94. Опишите процесс создания резервной копии пользовательского каталога.
95. Объясните принцип организации локальных и сетевых систем обнаружения атак
96. Дайте определение сетевых утилит.
97. Перечислите основные подходы к защите сети.
98. Опишите процесс настройки доступа к сетевым принтерам.
99. Объясните принцип организации распределенных систем обнаружения атак
100. Расскажите о функциях сетевых тест-программ.
101. Перечислите угрозы, связанные с преднамеренными ошибками.
102. Опишите процесс настроить параметры сети IPv4.
103. Объясните принцип организации систем обнаружения атак Snort

Практические задания.

1. Настройки DNS сервера. Установить программы Ethereal и подготовки к захвату.
2. Настройте одноранговую локальную сеть.
3. Настройте доступ к сетевым принтерам.
4. Настройте журналирование.
5. Настройте программу Ethereal. Произведите печать информации, просмотр кадра в отдельном окне.
6. Проанализируйте трафик сети на базе Lan2NET.
7. Разделите существующую сеть на подсети.
8. Настройте удалённый доступ к серверу.
9. Разрешить порт 1316 в брандмауэре.
- 10.Добавьте компьютера в домен.
- 11.Настройте ЛВС между тремя компьютерами.
- 12.Ограничте внешний трафик пользователю через панель управления Lan2NET.
- 13.Настройте подключение через ADSL модем.
- 14.На сервере под управлением windows server установите и настройте работу служб Active Directory, DHCP, RRAS, DNS.
- 15.С помощью программы архивации windows server выполните архивацию сервера.
- 16.Настроить прямую зону DNS Server