МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дагестанский государственный университет»

Колледж

УТВЕРЖДАЮ
директор Колледжа ДГУ
_____ Д.Ш. Пирбудагова
«31» 08 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

профессионального модуля

ПМ.01. ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Махачкала - 2021

Составитель/ составители:

Шахбанова М.И. - преподаватель кафедры естественно-научных и гуманитарных дисциплин Колледжа ФГБОУ ВО «Дагестанский государственный университет»

Шахбанова З.И. - к.э.н., доцент кафедры прикладной информатики в экономике факультета информатики и информационных технологий ФГБОУ ВО «Дагестанский государственный университет»

Фонд оценочных средств рассмотрен и рекомендован к утверждению на заседании кафедры специальных дисциплин колледжа ДГУ

Протокол №_1_ от «31» _____08_____2021г.

Зав. кафедрой _____/Магомедова А.М./

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

профессионального модуля

ПМ.01. ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
МДК.01.01. Эксплуатация автоматизированных систем в защищенном исполнении			
1.	**Раздел 1.** Разработка защищенных автоматизированных (информационных) систем	ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.2, ПК 1.3.	- устный опрос - тестирование - практические работы - самостоятельная работа
2.	**Раздел 2.** Эксплуатация защищенных автоматизированных систем.	ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.2, ПК 1.3.	- устный опрос - тестирование - практические работы - самостоятельная работа
3.	**Раздел 3.** Защита от несанкционированного доступа к информации в автоматизированных системах	ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.2, ПК 1.3.	- устный опрос - тестирование - практические работы - самостоятельная работа
МДК.01.02. Эксплуатация компьютерных сетей			
1.	**Раздел 1.** Основы передачи данных в компьютерных сетях	ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.2, ПК 1.3, ПК 1.4.	- устный опрос - тестирование - практические работы - самостоятельная работа
2.	**Раздел 2.** Технологии коммутации и маршрутизации современных сетей Ethernet	ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.2, ПК 1.3, ПК 1.4.	- устный опрос - тестирование - практические работы - самостоятельная работа

3.	**Раздел 3.** Межсетевые экраны	ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.2, ПК 1.3, ПК 1.4.	- устный опрос - тестирование - практические работы - самостоятельная работа
МДК.01.03. Сети и система передачи информации			
1.	**Раздел 1.** Общие сведения о сетях и системах передачи информации	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.1, ПК. 1.2.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
2.	**Раздел 2.** Уровни сетевого взаимодействия	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.1, ПК. 1.2.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
3.	**Раздел 3.** Построение локальной сети	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.1,	Комбинированный метод контроля в форме индивидуального,

		ПК. 1.2.	фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
4.	**Раздел 4.** Построение глобальной сети	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.1, ПК. 1.2.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
5.	**Раздел 5.** Защита информации в компьютерных сетях	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.1, ПК. 1.2.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных

			практических работ по решению ситуационных задач.
6.	**Раздел 6.** Техническая поддержка КС	ОК 1, ОК 2, ОК 3, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 1.1, ПК. 1.2.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
МДК.01.04. Антивирусная система			
1.	**Раздел 1.** Методы защиты от вирусов и других вредоносных программных объектов	ОК 1, ОК 2, ОК 3, ПК. 1.1, ПК. 1.2, ПК. 1.3.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
2.	**Раздел 2.** Методы защиты деструктивного воздействия	ОК 1, ОК 2, ОК 3, ПК. 1.1, ПК. 1.2, ПК. 1.3.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной

			работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	**2**	**3**	**4**
1.	Деловая и/или ролевая игра	Совместная деятельность группы обучающихся и педагогического работника под управлением педагогического работника с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Тема (проблема), концепция, роли и ожидаемый результат по каждой игре
2.	Кейс-задача	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы.	Задания для решения кейс-задачи
3.	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования педагогического работника с обучающимися.	Вопросы по темам/разделам дисциплин

			ы
4.	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Комплект контрольных заданий по вариантам
5.	Круглый стол, дискуссия, полемика, диспут, дебаты	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения.	Перечень дискуссионных тем.
6.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио
7.	Рабочая тетрадь	Дидактический комплекс, предназначенный для самостоятельной работы обучающегося и позволяющий оценивать уровень усвоения им учебного материала.	Образец рабочей тетради
8.	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умение обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированное аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.	Темы групповых и/или индивидуальных проектов
9.	Разно-уровневые задачи и задания	*Различают задачи и задания:* – репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; – реконструктивного уровня, позволяющие оценивать и диагностировать	Комплект разно-уровневых задач и заданий

		умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; – творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	
10.	Расчетно-графическая работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом.	Комплект заданий для выполнения расчетно-графической работы
11.	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Темы рефератов

КРИТЕРИИ ОЦЕНКИ
по дисциплине

МДК.01.01. ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Критерии оценки:

Оценка «отлично»: студент владеет знаниями предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивал при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи. Четко формирует ответы, решает ситуационные задачи повышенной сложности, хорошо знаком с основной литературой, увязывает теоретические аспекты предмета с задачами практического характера.

Оценка «хорошо»: студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах). Самостоятельно и отчасти при наводящих вопросах дает полноценные ответы, не всегда выделяет наиболее существенное, не допускает вместе с тем серьезных ошибок в ответах, умеет решать легкие и средней тяжести ситуационные задачи.

Оценка «удовлетворительно»: студент владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками. В процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.

Оценка «неудовлетворительно»: студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал, отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Вопросы к дифференцированному зачету и к экзамену по дисциплине «Эксплуатация автоматизированных систем в защищенном исполнении»:

1. Понятие автоматизированной (информационной) системы.
2. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС.
3. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность
4. Основные особенности современных проектов АИС. Электронный документооборот.
5. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные.
6. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение.
7. Модели жизненного цикла АИС.
8. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении.
9. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.
10. Требования к автоматизированной системе в защищенном исполнении.
11. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.
12. Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз.
13. Методы оценки опасности угроз. Банк данных угроз безопасности информации
14. Понятие уязвимости угрозы. Классификация уязвимостей.
15. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.
16. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним.
17. Идентификация и аутентификация субъектов доступа и объектов доступа.
18. Управление доступом субъектов доступа к объектам доступа.
19. Ограничение программной среды. Защита машинных носителей информации
20. Регистрация событий безопасности
21. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты.
22. Обновление баз данных признаков вредоносных компьютерных программ.

23. Обнаружение (предотвращение) вторжений
24. Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации.
25. Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.
26. Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных.
27. Резервное копирование и восстановление данных.
28. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.
29. Механизмы и методы защиты информации в распределенных автоматизированных системах.
30. Архитектура механизмов защиты распределенных автоматизированных систем.
31. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем
32. Общие требования по защите персональных данных.
33. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.
34. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.
35. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.
36. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.
37. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении
38. Анализ журнала аудита ОС на рабочем месте.
39. Построение сводной матрицы угроз автоматизированной (информационной) системы.
40. Анализ политик безопасности информационного объекта.
41. Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью.
42. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями.
43. Управление, тестирование и эксплуатация автоматизированных систем.
44. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
45. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.
46. Общие обязанности администратора информационной безопасности автоматизированных систем.

47. Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД.
48. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.
49. Классификация автоматизированных систем. Требования по защите информации от НСД для АС.
50. Требования защищенности СВТ от НСД к информации.
51. Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ.
52. Назначение и основные возможности системы защиты от несанкционированного доступа.
53. Архитектура и средства управления. Общие принципы управления.
54. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.
55. Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами.
56. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков.
57. Управление режимом контроля печати конфиденциальных документов.
58. Управление грифами конфиденциальности.
59. Обеспечение целостности информационной системы и информации
60. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.
61. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.
62. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации
63. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении
64. Основные эксплуатационные документы защищенных автоматизированных систем.
65. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем.
66. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.
67. Настройка и устранение неисправности программно- аппаратных средств защиты информации в компьютерных сетях по заданным правилам.

Правила выполнения практических работ:

При выполнении практических работ (ПР), студенты должны соблюдать и выполнять следующие правила:

1. Прежде, чем приступить к выполнению ПР, обучающийся должен подготовить ответы на теоретические вопросы к ПР.
2. Перед началом каждой работы проверяется готовность обучающегося к ПР.
3. После выполнения ПР студент должен представить отчет о проделанной работе в рабочей тетради или в собственном файле (в ПК) и подготовиться к обсуждению полученных результатов и выводов.
4. Студент (обучающийся), пропустивший выполнение ПР по уважительной или неуважительной причинам, обязан выполнить работу в дополнительно назначенное время.
5. Оценка за ПР выставляется с учетом предварительной подготовки к работе, доли самостоятельности при ее выполнении, точности и грамотности оформления отчета по работе.

Критерии оценки практических работ

Практические работы оцениваются по пятибалльной шкале.

Оценка «отлично»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, необходимые программы запущены и работают без ошибок; работа оформлена аккуратно;

Оценка «хорошо»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, частично с помощью преподавателя, присутствуют незначительные ошибки при запуске и эксплуатации (работе) необходимых программ; работа оформлена аккуратно;

Оценка «удовлетворительно»: частично с помощью преподавателя, присутствуют ошибки при запуске и работе требуемых программ; по оформлению работы имеются замечания.

Оценка «неудовлетворительно»: ставится, если обучающийся не подготовился к ПР, при запуске и эксплуатации (работе) требуемых программ студент допустил грубые ошибки, по оформлению работы имеются множественные замечания.

Примерный перечень практических заданий:

Практическая работа №1

Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)

Задание

1. Рассмотреть компоненты информационной системы: база данных (БД); схема базы данных;
2. Система управления базой данных (СУБД); приложения; пользователи; технические средства.
3. Найти информацию, характеризующую назначение и область применения заданного вида информационных систем.
4. Определить, к какому классу относится заданный вид информационных систем (по характеру использования информации, по сфере применения, по способу организации, по уровню и масштабу решаемых задач).
5. Составить общее описание заданного вида информационных систем.
6. Найти описание нескольких (не менее двух) современных информационных систем, относящихся к заданному виду.
7. Сформулировать краткое описание назначения и функциональных возможностей каждой из информационных систем по отдельности. Указать на характеристики и свойства, которые являются общими для всех рассматриваемых ИС.
8. Составить таблицу отличий между информационными системами.
9. Указать на их индивидуальные особенности, различающиеся количественные и качественные характеристики.
10. Разработать пример возможного применения одной из информационных систем в деятельности некоторого объекта автоматизации (предприятия или организации). Вид деятельности объекта автоматизации выбирается самостоятельно.
11. Составить документ-обоснование для внедрения информационной системы. Описать, чего позволит достичь внедрение информационной системы с точки зрения повышения эффективности работы объекта автоматизации (организации, предприятия). 1580436089

Результаты зафиксировать в отчете.

Практическая работа №2

Разработка технического задания на проектирование автоматизированной системы

Задание

Для создания пояснительной записки использовать MS Word, а для создания схем и диаграмм рекомендуется использовать MS Visio.

1. Ознакомиться с примером технического задания для разработки какой-либо автоматизированной системы (АС), изучить основные типовые его разделы, ГОСТ 34.602-89
2. Необходимо для себя ответить на следующие вопросы:
    а) на основании каких документов разрабатывается методическое и информационное обеспечение системы (нормативные и другие документы);
    б) перечень исходных данных: - какие массивы данных используются и в каких форматах; - на каких носителях эти данные будут поставляться в систему;
    в) перечень выходных данных: - какие массивы данных будут являться результатом работы ПС; - какие документы будут представлены пользователю и в каком виде (указывается вид носителя) и с какой периодичностью; - какие требования по целостности данных и их защите должны быть выполнены в проектируемой системе.
3. Используя пример и ГОСТ в пояснительной записке технического задания сформировать и описать раздел «Характеристика объекта управления»
4. Сформировать и описать раздел «Назначение АС»
5. Сформировать и описать раздел «Основные требования к АС»
6. Сформировать и описать раздел «Технико-экономические показатели АС»
7. Сформировать и описать раздел «Состав, содержание и организация работ по созданию АС»
8. Сформировать и описать раздел «Порядок приемки АС»

Результаты зафиксировать в отчете

Практическая работа №3

Построение модели угроз

Задание

1. Получить у преподавателя описание.
2. Для данной ИС построить модель угроз и уязвимостей:
    - выделить уязвимости, через которые могут быть реализованы угрозы;
    - определить угрозы, которые могут воздействовать на каждый из ресурсов в рамках ИС, и обосновать
      причины наличия этих угроз;
      выделить угрозы, применимые к рассматриваемой ИС;
    - определить уязвимости, через которые могут быть реализованы указанные угрозы.

Содержание отчета

1. Формулировка задачи.
2. Описание построенной модели угроз и уязвимостей.

Предметная область.

Тестовая информационная система ЗАО "ТестИС-Строй".

Основной вид деятельности ЗАО "ТестИС-Строй" – продажа строительных товаров на рынке "BusinesstoClient". Поставщиками являются частные лица и организации среднего и малого бизнеса. ЗАО "ТестИС-Строй" имеет четыре точки продаж, расположенные в пределах города. Каждая из этих точек – магазин площадью от 300 до2000 м2. В каждом магазине работает до 100 сотрудников.

ЗАО "ТестИС-Строй" имеет центральный офис в центре города, где располагается дата-центр, включающий центральную базу данных товаров и серверы баз данных бухгалтерии, отдела кадров и т. д. В центральном офисе и на каждой из точек продаж развернуты локальные вычислительные сети (ЛВС).

Каждая из ЛВС точек продаж связана с центральным офисом посредством сети Интернет. В точках продаж функционируют 1-2 сервера, обеспечивающих синхронизацию с центральной базой данных, и до 20 рабочих станций: компьютеры директора магазина, секретаря, терминалы в торговых залах.

В дата-центре установлены Web-сайт электронного магазина и почтовый сервер.

К терминалам торговых залов исключена возможность подключения внешних носителей. В датацентре все серверы размещены в несгораемых сейфах, доступ в помещение контролируется физически(охраняемое помещение). В торговых точках все серверы находятся в кабинетах, закрываемых на ключ. На всех компьютерах, кроме терминалов в торговых залах, установлено антивирусное ПО.

На серверах дата-центра установлен межсетевой экран. На сервере базы данных бухгалтерии дополнительно установлена система обнаружения вторжений.

Для подключения к дата-центру используется защищенноеVPN-соединение. Для подключения к центральной базе товаров предусмотрен резервный канал. Загрузка терминалов торговых залов обеспечивается только после введения пароля в BIOS.

Примерные задачи по дисциплине:

1. Разработать модель разрешительной системы ролевого управления доступом в автоматизированной системе, с учетом:
   - групп пользователей (не более 5 ролей);
   - выполняемых функций группами пользователей;
   - наименования информационного ресурса;
   - меток конфиденциальности информационного ресурса;
   - мест хранения информационного ресурса (каталог HDD);
   - прав на доступ к информации (R - чтение, W - запись, D - удаление, N переименование, E - исполнение, M - модификация, A - полный доступ).

2. Разработать частную модель угроз безопасности распределенной информационной системы персональных данных (ИС ПДн) с подключением к сети международного информационного обмена по следующим исходным данным:
   - локальная ИС ПДн, развернута в пределах нескольких близко расположенных зданий;
   - имеет многоточечный выход в сеть общего пользования;
   - позволяет запись, удаление, сортировку ПДн;
   - имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн;
   - используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн;
   - данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;
   - предоставляются сторонним пользователям ИС ПДн без предварительной обработки только часть ПДн.
3. Определить уровень базовый уровень защищенности ИС ПДн по следующим исходным данным:
   - обработка ПДн сотрудников организации;
   - категории биометрических и иных персональных данных;
   - объем обработки менее 100000 субъектов персональных данных;
   - возможны угрозы 2 типа.
4. Определить состав и содержание организационных и технических мер по защите ИС ПДн в соответствии с уровнем защищенности, руководствуясь последовательностью действий:
   - определить базовый набор мер для третьего уровня защищенности ПДн;
   - адаптировать базовый набор мер, с учетом характеристик распределенной информационной системы;
   - подготовить предложения для уточнения адаптированного базового набора мер для различных вариантов ИС ПДн.

Подобрать необходимый для заданного уровня защищенности ПДн состав средств защиты информации.

5. Разработать структуру технического задания на создание автоматизированной системы в защищенном исполнении. Составить технический паспорт на автоматизированную систему в защищенном исполнении, включающий:
   - общие сведения об автоматизированной системе;
   - состав оборудования автоматизированной системы (состав основных и вспомогательных средств и систем);
   - состав средств защиты информации.

Курсовая работа (проект) является формой промежуточной аттестации обучающихся по дисциплине **«Эксплуатация автоматизированных систем в защищенном исполнении»**

Курсовая работа (проект) выполняется обучающимися с целью:

1. формирования навыков применения теоретических знаний, полученных в ходе освоения дисциплины;
2. формирования практических навыков в части сбора, анализа и интерпретации результатов, необходимых для последующего выполнения научных научно-исследовательской работы;
3. формирования навыков логически и последовательно иллюстрировать подготовленную в процессе выполнения курсовой работы информацию;
4. формирования способностей устанавливать закономерности и тенденции развития явлений и процессов , анализировать , обобщать и формулировать выводы;
5. формировать умение использовать результаты, полученные в ход е выполнения курсовой работы в профессиональной деятельности.

Критерии оценивания курсовой работы:

Оценка «отлично»: исчерпывающее или достаточное изложение содержания тематики курсовой работы в пояснительной записке, соответствие структуры постельной записки курсовой работы установленным требованиям, уверенное изложение тематики курсовой работы в ходе процедуры защиты, верные ответы на заданные педагогическим работником вопросы.

Оценка «хорошо»: исчерпывающее но не достаточное изложение содержания тематики курсовой работы в пояснительной записке, незначительное не соответствие структуры постельной записки курсовой работы установленным требованиям, неуверенное изложение тематики курсовой работы в ходе процедуры защиты, верные ответы на заданные педагогическим работником вопросы.

Оценка «удовлетворительно»: недостаточное изложение содержания тематики курсовой работы в пояснительной записке, нарушение структуры пояснительной записки курсовой работы установленным требованиям, неуверенное изложение тематики курсовой работы в ходе процедуры защиты, верный ответ на один или отсутствие верных ответов на оба вопроса, или курсовая работа(проект) не представлена к проверке и защите.

Оценка «неудовлетворительно»: курсовая работа (проект) не выполнена.

Примерная тематика курсовой работы по дисциплине **«Эксплуатация автоматизированных систем в защищенном исполнении»:**

1. Физическое кодирование с использованием манчестерского кода
2. Логическое кодирование с использованием скремблирования
3. Подключение клиента к беспроводной сети в инфраструктурном режиме
4. Оценка беспроводной линии связи
5. Проектирования беспроводной сети
6. Сбор информации о клиентских устройствах
7. Планирование производительности и зоны действия беспроводной сети
8. Предпроектное обследование места установки беспроводной сети
9. Обеспечение отказоустойчивости в беспроводных сетях
10. Режимы работы и организация питания точек доступа
11. Сегментация беспроводной сети
12. Настройка QoS
13. Постпроектное обследование и тестирование сети
14. Создание ACL-списка
15. Наблюдение за трафиком в сети VLAN
16. Определение уязвимых мест сети
17. Реализация функций обеспечения безопасности порта коммутатора
18. Исследование трафика
19. Создание структуры сети организации
20. Определение технических требований
21. Мониторинг производительности сети
22. Создание диаграммы логической сети
23. Подготовка к обследованию объекта
24. Обследование зоны беспроводной связи
25. Формулировка общих целей проекта
26. Разработка требований к сети
27. Анализ существующей сети
28. Определение характеристик сетевых приложений
29. Анализ сетевого трафика
30. Определение приоритетности трафика
31. Изучение качества обслуживания сети
32. Исследование влияния видеотрафика на сеть
33. Определение потоков трафика, построение диаграмм потоков трафика
34. Применение проектных ограничений
35. Определение проектных стратегий для достижения масштабируемости
36. Определение стратегий повышения доступности
37. Определение требований к обеспечению безопасности
38. Разработка ACL-списков для реализации наборов правил межсетевого экрана
39. Использование CIDR для обеспечения объединения маршрутов
40. Определение схемы IP-адресации
41. Определение количества IP-сетей

42. Создание таблицы для выделения адресов
43. Составление схемы сети
44. Анализ плана тестирования и выполнение теста
45. Создание плана тестирования для сети комплекса зданий
46. Проектирование виртуальных частных сетей
47. Безопасная передача данных в беспроводных сетях

Критерии оценки эссе (рефератов, докладов, сообщений) по дисциплине «Эксплуатация автоматизированных систем в защищенном исполнении»

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений):

1. Разработка концепции защиты автоматизированной (информационной) системы.
2. Анализ банка данных угроз безопасности информации
3. Анализ журнала аудита ОС на рабочем месте.

4. Построение сводной матрицы угроз автоматизированной (информационной) системы.
5. Анализ политик безопасности информационного объекта
6. Изучение аналитических обзоров в области построения систем безопасности.
7. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации.
8. Настройка Wi-Fi маршрутизатора.
9. Изучение сетевых утилит.
10. Конфигурирование сетевого интерфейса
11. Маршрутизация и управление потоками в сетях связи.
12. Разработка концепции защиты автоматизированной (информационной) системы.
13. Анализ банка данных угроз безопасности информации
14. Анализ журнала аудита ОС на рабочем месте.
15. Построение сводной матрицы угроз автоматизированной (информационной) системы.
16. Анализ политик безопасности информационного объекта
17. Изучение аналитических обзоров в области построения систем безопасности.
18. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования.
19. Физическое кодирование с использованием манчестерского кода.
20. Логическое кодирование с использованием скремблирования.
21. Подключение клиента к беспроводной сети в инфраструктурном режиме.
22. Оценка беспроводной линии связи.
23. Проектирования беспроводной сети.
24. Сбор информации о клиентских устройствах.
25. Планирование производительности и зоны действия беспроводной сети.
26. Предпроектное обследование места установки беспроводной сети.
27. Обеспечение отказоустойчивости в беспроводных сетях.
28. Режимы работы и организация питания точек доступа.
29. Сегментация беспроводной сети.
30. Настройка QoS.
31. Постпроектное обследование и тестирование сети.
32. Создание ACL-списка.
33. Наблюдение за трафиком в сети VLAN.

СТРУКТУРА ИТОГОВОГО ТЕСТА:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования

MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Эксплуатация автоматизированных систем в защищенном исполнении»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	**Оценка знаний**
90-100	5 «отлично»
75-89	4 «хорошо»
60-74	3 «удовлетворительно»

Менее 60	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ) по дисциплине «Эксплуатация автоматизированных систем в защищенном исполнении»

1. Основы информационных систем как объекта защиты.

Выберите правильную последовательность уровней защиты информационной системы:

а) пользовательский -сетевой -локальный -технологический -физический
б) пользовательский -технологический -физический-сетевой -локальный
в) локальный -технологический -физический -пользовательский –сетевой

2. Для чего создаются информационные системы?
   а) получения определенных информационных услуг
   б) обработки информации
   в) все ответы правильные
3. Какие трудности возникают в информационных системах при конфиденциальности?
   а) сведения о технических каналах утечки информации являются закрытыми
   б) на пути пользовательской криптографии стоят многочисленные технические проблемы
   в) все ответы правильные
4. Основными источниками внутренних отказов информационных систем являются:
   а) ошибки при конфигурировании системы
   б) отказы программного или аппаратного обеспечения
   в) выход системы из штатного режима эксплуатации
5. Утечкой информации в информационной системе называется ситуация, характеризуемая:
   а) потерей данных в системе 1580436089
   б) изменением формы информации
   в) изменением содержания информации
6. Угроза информационной системе (компьютерной сети) – это:
   а) вероятное событие
   б) детерминированное (всегда определенное) событие
   в) событие, происходящее периодически

8. Политика безопасности в информационной системе (сети) – это комплекс:
   а) руководств, требований обеспечения необходимого уровня безопасности
   б) инструкций, алгоритмов поведения пользователя в сети
   в) нормы информационного права, соблюдаемые в сети

9. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она:
   а) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
   б) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации способна противостоять только информационным угрозам, как внешним так и внутренним способна противостоять только внешним информационным угрозам
10. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности:
   а) Оранжевая книга
   б) Закон «Об информации, информационных технологиях и о защите информации»
   в) рекомендации X.800
11. Базовые модели жизненного цикла: (выбрать все верные)
   а) каскадная модель
   б) поэтапная модель
   в) логическая модель
   г) спиральная модель
   д) интеллектуальная модель
12. Непрерывный процесс, который начинается с момента принятия решения о необходимости создания ИС и заканчивается в момент ее полного изъятия из эксплуатации это:
   а) разработка
   б) жизненный цикл
   в) конфигурация
   г) управление проектами
13. Что входит в структуру ЖЦ по стандарту ISO/IEC:
   а) организационные процессы
   б) основные процессы ЖЦ
   в) дополнительные процессы
   г) ветвящиеся процессы
14. Структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач, выполняемых на протяжении ЖЦ это:
   а) проект
   б) модель ЖЦ
   в) инструкция
   г) 1580436089
15. Технологии, базирующиеся на методологиях подготовки информационных систем и соответствующих комплексах

интегрированных инструментальных средств, а также ориентированные на поддержку полного жизненного цикла АС или его основных этапов это:

а) nano-технологии
б) CASE-технологии
в) инновационные технологии
г) информационные технологии

16. В стандарте ISO 12207 описаны ____ основных процессов жизненного цикла программного обеспечения

а) три
б) четыре
в) пять
г) шесть

17. ISO 12207 – базовый стандарт процессов жизненного цикла

а) программного обеспечения
б) информационных систем
в) баз данных
г) компьютерных систем

18. Согласно ISO 12207, процессы, протекающие во время жизненного цикла программного обеспечения, должны быть совместимы с процессами, протекающими во время жизненного цикла

а) автоматизированной системы
б) информационной системы
в) компьютерной системы
г) системы обработки и передачи данных

19. Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является

а) приобретение
б) решение проблем
в) обеспечение качества
г) аттестация

20. Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является

а) процесс поставки
б) документирования
в) аудит
г) управление конфигурацией

21. Источник угрозы информационной безопасности для автоматизированных систем – это:

а) потенциальный злоумышленник
б) злоумышленник
в) нет правильного ответа

22. Угрозы ИБ в автоматизированных системах можно классифицировать по нескольким критериям:

а) по спектру ИБ

б) по способу осуществления
в) по компонентам АИС

23. По каким компонентам классифицируется угрозы доступности в автоматизированных системах:
    а) 1580436089
    б) отказ пользователей
    в) отказ поддерживающей инфраструктуры
    г) ошибка в программе
24. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
    а) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
    б) обрабатывать большой объем программной информации
    в) нет правильного ответа
25. Вид источника угрозы ИБ, характер возникновения которого обусловлен действиями субъекта:
    а) техногенный источник
    б) антропогенный источник
    в) стихийный источник.
26. Степень квалификации и привлекательность совершения деяний со стороны источника угрозы (для антропогенных источников), или наличие необходимых условий (для техногенных и стихийных источников):
    а) готовность источника
    б) фатальность
    в) возможность возникновения источника
27. Естественные угрозы безопасности информации в АИС вызваны:
    а) ошибками при действиях персонала
    б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
    в) воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека
    г) корыстными устремлениями злоумышленников
28. Угрозы ИБ, реализация которых не влечет за собой изменение структуры данных (копирование):
    а) естественные угрозы
    б) пассивные угрозы
    в) активные угрозы
    г) искусственные угрозы
29. По каким критериям нельзя классифицировать угрозы:
    а) по расположению источника угроз
    б) по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
    в) по способу предотвращения
    г) по компонентам информационных систем, на которые угрозы нацелены

30. Наиболее распространены угрозы информационной безопасности корпоративной системы:
    а) покупка нелицензионного ПО
    б) ошибки эксплуатации и неумышленного изменения режима работы системы
    в) сознательного внедрения сетевых вирусов
31. Защита информации от несанкционированного доступа - это деятельность по предотвращению:
    а) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.
    б) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.
    в) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
32. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
    а) анализ рисков
    б) анализ затрат / выгоды
    в) результаты ALE
33. Какие меры по защите информации в автоматизированных системах дают наибольший эффект?
    а) организационные
    б) технические (аппаратные)
    в) программные
    г) все в совокупности
    д) правильных ответов нет
34. Требования к программному обеспечению АСЗИ включают в себя требования: (выбрать все верные)
    а) к алгоритму принятия решения;
    б) к системе классификации;
    в) к системе команд;
    г) к алгоритму обработки событий;
    д) к сертификации программного обеспечения;
    е) к системе диагностики программного обеспечения.
    ж) к оптимизации кода программного обеспечения и средству разработки
    з) 1580436089

Основные литература:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1: учебник и практикум для среднего профессионального образования / М. В. Дибров. -Москва : Издательство Юрайт, 2022. -333 с. -(Профессиональное образование). -ISBN 978-5-534-04638-0. -URL : https://urait.ru/bcode/491456
2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2: учебник и практикум для среднего профессионального образования / М. В. Дибров. -Москва : Издательство Юрайт, 2022. -351 с. -(Профессиональное образование). -ISBN 978-5-534-04635-9. -URL : https://urait.ru/bcode/491951
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. -Москва : Издательство Юрайт, 2021. -312 с. -(Профессиональное образование). -ISBN 978-5-534-13221-2. -URL : https://urait.ru/bcode/476997

Дополнительная литература:

1. Дибров М.В. Компьютерные сети и телекоммуникации. Маршрутизация в IP – сетях. В 2ч. Часть 1: учебник и практикум для СПО М.: Издательство Юрайт, 2020
2. Карпов В.Е., Коньков К.А. Основы операционных систем. Практикум Интуит НОУ, 2020
3. Коньков К.А., Карпов В.Е. Основы операционных систем. Интуит НОУ, 2016
4. Коньков К.А. Основы организации операционных систем Microsoft Windows Интуит НОУ, 2016

Интернет-ресурсы:

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

КРИТЕРИИ ОЦЕНКИ

по дисциплине

МДК.01.02. ЭКСПЛУАТАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Критерии оценки:

Оценка «отлично»: студент владеет знаниями предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивал при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи. Четко формирует ответы, решает ситуационные задачи повышенной сложности, хорошо знаком с основной литературой, увязывает теоретические аспекты предмета с задачами практического характера.

Оценка «хорошо»: студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах). Самостоятельно и отчасти при наводящих вопросах дает полноценные ответы, не всегда выделяет наиболее существенное, не допускает вместе с тем серьезных ошибок в ответах, умеет решать легкие и средней тяжести ситуационные задачи.

Оценка «удовлетворительно»: студент владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками. В процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.

Оценка «неудовлетворительно»: студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал, отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Вопросы к дифференцированному зачету по дисциплине «Эксплуатация компьютерных сетей»:

1. Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.
2. Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.
3. Изучение элементов кабельной системы.
4. Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.
5. Методы совместного использования среды передачи канала связи.
6. Мультиплексирование и методы множественного доступа.
7. Оптоволоконные линии связи. Стандарты кабелей. Электрическая проводка.
8. Беспроводная среда передачи. Создание сетевого кабеля на основе неэкранированной витой пары (UTP). Сварка оптического волокна
9. Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.
10. Разработка топологи сети небольшого предприятия. Построение одноранговой сети.
11. Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.
12. Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI.
13. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.
14. Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети.
15. Технология PoweroverEthernet
16. Создание коммутируемой сети. Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.
17. Маршрутизация пакетов IPv4. Протоколы динамической маршрутизации
18. Сеть FDDI. Сеть 100VG-AnyLAN. Сверхвысокоскоростные сети. Беспроводные сети.
19. Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов.
20. Управление потоком в полудуплексном и дуплексном режимах.
21. Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов
22. Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.
23. Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор.
24. Загрузка и резервное копирование конфигурации коммутатора.
25. Команды управления таблицами коммутации MAC- и IP- адресов, ARP-таблицы

26. Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.
    Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation. Настройка VLAN на основе стандарта IEEE 802.1Q
27. Настройка протокола GVRP. Настройка сегментации трафика без использования VLAN.
28. Настройка функции Q-in-Q (Double VLAN).
29. Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.
30. Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.
31. Дополнительные функции защиты от петель. Агрегирование каналов связи.
32. Настройка протоколов связующего дерева STP, RSTP, MSTP.
33. Настройка функции защиты от образования петель LoopBackDetection
34. Агрегирование каналов.
35. Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.
36. Протокол IPv6. Формирование идентификатора интерфейса.
37. Способы конфигурации IPv6-адреса.
38. Планирование подсетей IPv6. Протокол NDP.
39. Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.
40. Тематика практических занятий и лабораторных работ
41. Основные конфигурации маршрутизатора.
42. Расширенные конфигурации маршрутизатора.
43. Работа с протоколом CDP.
44. Работа с протоколом TELNET. Работа с протоколом TFTP.
45. Работа с протоколом RIP.
46. Работа с протоколом OSPF.
47. Конфигурирование функции маршрутизатора NAT/PAT.
48. Конфигурирование PPP и CHAP.
49. Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.
50. Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок.
51. Контроль полосы пропускания. Пример настройки QoS.
52. Настройка QoS. Приоритизация трафика. Управление полосой пропускания
53. Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.
54. Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.
55. Списки управления доступом (AccessControlList)
56. Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.

57. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding
58. Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.
59. Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI
60. (IGMP Snooping).Функция IGMP FastLeave.
61. Отслеживание трафика многоадресной рассылки.
62. Отслеживание трафика Multicast.
63. Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.
64. Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны.
65. Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.
66. Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.
67. Основы администрирования межсетевого экрана
68. Соединение двух локальных сетей межсетевыми экранами
69. Создание политики без проверки состояния.
70. Создание политик для традиционного (или исходящего) NAT.
71. Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing
72. Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.
73. Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.
74. Обнаружение и предотвращение вторжений.
75. Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.
76. Создание альтернативных маршрутов с использованием статической маршрутизации

Правила выполнения практических работ:

При выполнении практических работ (ПР), студенты должны соблюдать и выполнять следующие правила:

6. Прежде, чем приступить к выполнению ПР, обучающийся должен подготовить ответы на теоретические вопросы к ПР.
7. Перед началом каждой работы проверяется готовность обучающегося к ПР.
8. После выполнения ПР студент должен представить отчет о проделанной работе в рабочей тетради или в собственном файле (в ПК) и подготовиться к обсуждению полученных результатов и выводов.

9. Студент (обучающийся), пропустивший выполнение ПР по уважительной или неуважительной причинам, обязан выполнить работу в дополнительно назначенное время.
10. Оценка за ПР выставляется с учетом предварительной подготовки к работе, доли самостоятельности при ее выполнении, точности и грамотности оформления отчета по работе.

Критерии оценки практических работ

Практические работы оцениваются по пятибалльной шкале.

Оценка «отлично»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, необходимые программы запущены и работают без ошибок; работа оформлена аккуратно;

Оценка «хорошо»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, частично с помощью преподавателя, присутствуют незначительные ошибки при запуске и эксплуатации (работе) необходимых программ; работа оформлена аккуратно;

Оценка «удовлетворительно»: частично с помощью преподавателя, присутствуют ошибки при запуске и работе требуемых программ; по оформлению работы имеются замечания.

Оценка «неудовлетворительно»: ставится, если обучающийся не подготовился к ПР, при запуске и эксплуатации (работе) требуемых программ студент допустил грубые ошибки, по оформлению работы имеются множественные замечания.

Примерная тематика практических работ по дисциплине «Эксплуатация компьютерных сетей»:

Практическая работа №1 Установка офисного приложения Microsoft Office в операционной системе Windows

Практическая работа №2 Создание базы данных в программе Access Microsoft Office и выполнение запроса на языке SQL

Практическая работа №3 Создание учетной записи, отправка и получение писем с помощью программы Outlook Microsoft Office

Практическая работа №4 Установка офисного приложения LibreOffice в операционной системе Linux

Практическая работа №5 Создание документов в приложении Writer LibreOffice

Практическая работа №6 Создание таблиц в приложении Calc LibreOffice

Практическая работа №7 Создание графических изображений в приложении Draw LibreOffice

Практическая работа №8 Создание базы данных в приложении Base LibreOffice

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений) по дисциплине «Эксплуатация компьютерных сетей»:

1. Разработка проекта по администрированию сервера Active Directory для промышленного предприятия.
2. Реализация доступа к локальным и глобальным сетям на предприятии.
3. Сети ЭВМ и телекоммуникации.
4. Моделирование процессов размножения и гибели популяции
5. Сети ЭВМ и телекоммуникации.
6. Управление сетями связи.

7. Проектирование локальной вычислительной сети организации.
8. Модель взаимодействия открытых систем (OSI) ISO
9. Семейство протоколов IEEE 802.11 (WiFi)
10. Стек протоколов TCP/IP v4
11. Протокол IPv6
12. Технология Network Address Translation
13. Динамическая маршрутизация
14. Автономные системы и маршрутизация в Internet
15. Протокол BitTorent
16. TOR (The Onion Router)
17. Развитие сетей связи.
18. Эталонная модель взаимодействия открытых систем OSI.
19. Организации стандартизации в области телекоммуникаций.
20. Линии связи на основе симметричных кабелей.
21. Линии связи на основе коаксиальных кабелей.
22. Линии связи на основе волоконно-оптических кабелей.
23. Источники оптического излучения: лазеры, светодиоды и пр.
24. Фотоприемники.
25. Оптические компоненты.
26. Структурированные кабельные системы SCS.
27. Устройство и принцип действия аналоговых и цифровых телефонных аппаратов.
28. Система сигнализации №7 (SS7).
29. Транзит SS7 по IP-сетям.
30. Конверторы сигнализации.
31. Особенности распространения радиоволн различных диапазонов.
32. Антенны.Радиорелейные системы передачи.
33. Беспроводные абонентские линии (Radio in Local Loop).
34. Системы спутниковой связи.
35. Низкоорбитальные спутниковые системы.
36. Непосредственное телевизионное вещание с ИСЗ.
37. Глобальные системы определения координат GPS и ГЛОНАСС.
38. Стандарты телевидения PAL, SECAM, NTSC.
39. Цифровое телевидение.
40. Телевидение высокой четкости HDTV.
41. Стандарты сжатия видеосигналов.
42. Сотовые системы подвижной связи.
43. Стандарт GSM.
44. Стандарт CDMA.
45. Системы персонального радиовызова (пейджинг).
46. Транкинговые системы связи.
47. Системы беспроводных телефонов
48. Технология асинхронного режима доставки ATM.
49. Эмуляция локальных сетей (ATM LANE).
50. ATM-коммутация.

51.Интерфейсы ATM.
52.Передача изображений в сетях ATM (Video over ATM)
53. Передача речевых сигналов в сетях ATM (VTOA).
54.Сети Ethernet. Fast Ethernet..
55. Язык гипертекстовой разметки HTML.
56.World Wide Web.
57.Протоколы управления сетью SNMP и CMIP.
58.Стандарт RMON.
59.Передача речевых сигналов в IP-сетях (Voice over IP).
60.Передача изображений в IP-сетях (Video over IP).
61.Обеспечение качества обслуживания (QoS) в сетях передачи данных.
62.Протокол резервирования ресурсов RSVP в IP сетях
63.Развитие сетей ТФОП в России.
64.Развитие сетей ISDN в России.

СТРУКТУРА ИТОГОВОГО ТЕСТА:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических

работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Эксплуатация компьютерных сетей»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	Оценка знаний
90-100	5 «отлично»
75-89	4 «хорошо»
60-74	3 «удовлетворительно»
Менее 60	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ) по дисциплине «Эксплуатация компьютерных сетей»:

1. Главное требование, предъявляемое к сетям:
    а) Выполнение сетью ее основной функции – обеспечение пользователям потенциальной возможности доступа к разделяемым ресурсам всех ПК, объединенных в сеть.
    б) Объединение территориально рассредоточенных компьютеров, которые могут находиться в различных городах и странах.
    в) Связь локальных сетей в масштабах города и соединение локальных сетей с глобальными.
2. Концепция соединенных и совместно использующих ресурсы компьютеров называется:
    а) локальной сетью
    б) сетевым взаимодействием
    в) глобальной сетью
3. Серверы:
    а) компьютеры, осуществляющие доступ к сетевым ресурсам.
    б) компьютеры, предоставляющие свои ресурсы сетевым пользователям.
    в) способ соединения компьютеров.
4. Клиенты:

а) компьютеры, осуществляющие доступ к сетевым ресурсам.
б) компьютеры, предоставляющие свои ресурсы сетевым пользователям.

5. Способ соединения компьютеров.
   а) компьютеры, осуществляющие доступ к сетевым ресурсам.
   б) компьютеры, предоставляющие свои ресурсы сетевым пользователям.
6. В формуле для эффективной девиации частоты системы передачи с частотным разделением каналов: $\Delta f_{эф} = 0,224\Delta f_K\sqrt{N}$, N > 240 через N обозначен (о)
   а) число стволов системы передачи
   б) индекс частотной модуляции
   в) номер наивысшей частоты
   г) число каналов системы передачи
7. Группа соединенных средой передачи компьютеров и других устройств на ограниченной территории и работающих в интерактивном режиме.
   а) городская сеть.
   б) ГВС (глобальная вычислительная сеть).
   в) ЛВС (локальная вычислительная сеть).
8. Рекомендуемое значение номера прерывания для ПСА:
   а) IRQ 7
   б) IRQ 5
   в) IRQ 3
9. В Project 802 модели OSI разделен на два подуровня уровень:
   а) канальный
   б) физический
   в) прикладной
10. Протоколы разделены на три типа, соответствующие модели OSI: прикладной, сетевой и:
    а) физический
    б) транспортный
    в) канальный
11. Обычно содержит информацию для проверки ошибок, называемую CRC:
    а) заголовок пакета
    б) трейлер
    в) данные
12. Параллельный порт:
    а) наибольшее пространство между фальш – потолком и перекрытием.
    б) поддерживает передачу речи, данных и видео.
    в) обычно использует irq 7.
12. В модели OSI все сетевые операции разделены на уровней:
    а) 7.
    б) 14.
    в) 2.

13. Процесс создания пакета начинается на уровне модели OSI:
    а) представительском
    б) прикладном
    в) транспортном
14. Драйвер:
    а) аппаратное обеспечение.
    б) программное обеспечение.
    в) периферийное устройство.
15. Какой протокол является протоколом Сетевого уровня:
    а) IPX.
    б) Telnet.
    в) FTP.
16. Какой метод доступа используется при прослушивании кабеля перед отправкой данных, чтобы определить присутствие трафика:
    а) CSMA/CD.
    б) CSMA/CA.
    в) С передачей маркера.
17. ArcNet
    а) использует топологию звезда - шина на базе utp
    б) использует передачу маркера и топологию звезда - шина
    в) использует передачу маркера и топологию шина
18. 10 BaseT
    а) использует топологию звезда - шина на базе UTP
    б) использует передачу маркера и топологию звезда - шина
    в) использует передачу маркера и топологию шина
19. Token Ring
    а) используется в среде SNA.
    б) сочетает Token Ring и Ethernet.
    в) использует передачу маркера и топологию шина.
20. 100 BaseX
    а) известна как Fast Ethernet
    б) использует передачу маркера и топологию шина
    в) использует топологию шина на базе кабеля тонкий Ethernet
21. LocalTalk
    а) встроенное в Macintosh сетевое программное обеспечение.
    б) использует топологию шина на базе кабеля толстый Ethernet.
    в) использует передачу маркера и топологию шина.
22. Какой тип сети можно использовать между двумя зданиями:
    а) оптоволоконный Ethernet
    б) щптоволоконный Token Ring
    в) Ethernet 10 Base2.
23. Какой тип сети следует принять в качестве стандарта для прокладки в офисах:
    а) оптоволоконный Ethernet
    б) оптоволоконный Token Ring

в) Ethernet 10 BaseT.

24. Гибкая сетевая архитектура, для ЛВС масштаба рабочих групп, категории IEEE 802.4:
    а) Token Ring.
    б) ArcNet.
    в) Ethernet.
25. Переадресует запросы с одного компьютера на другой:
    а) спулер.
    б) редиректор.
    в) язык описания страниц (PDL).
26. Буфер в оперативной памяти сервера печати:
    а) спулер.
    б) редиректор.
    в) язык описания страниц (PDL).
27. Прикладные программы сетевой операционной системы, приводящие сеть в действие:
    а) связи.
    б) службы.
    в) SQL
28. Иерархия протоколов от верхних уровней модели **OSI** к нижним уровням:
    а) связи.
    б) службы.
    в) SQL
29. Стандарты, включающие агентов пользователя и агентов передачи сообщений:
    а) X.400.
    б) X.500.
    в) MHS.
30. Службы каталогов, помогающие найти пользователей в распределенной сети для передачи им сообщений электронной почты:
    а) X.400.
    б) X.500.
    в) MHS.
31. Часть протокольного стека TCP/IP, используемая для передачи сообщений между двумя удаленными сетевыми компьютерами:
    а) SMTR.
    б) SQL.
    в) X.500.
32. Разработан IBM для обеспечения относительно простого метода манипулирования данными:
    а) SMTR.
    б) SQL.
    в) X.500.
33. Основные методы построения клиент – серверных сетей:
    а) данные располагаются на одном сервере.

б) данные распределяются между несколькими серверами.
в) данные располагаются на одном сервере, и данные распределяются между несколькими серверами.

34. Сервер в клиент – серверной среде предназначен:
а) для обновления и добавления данных.
б) для защиты и обновления данных.
в) для хранения и управления данными.

35. Стандарт помогающий пользователям находить в распределенных сетях пользователей для обмена сообщениями:
а) X.400.
б) X.500.
в) SMTP.

36. UA, MTA, MTS компоненты какого стандарта:
а) X.400.
б) X.500.
в) SMTP.

37. Модем преобразует цифровой сигнал ПК в аналоговый на стороне:
а) принимающей.
б) передающей.
в) принимающей и передающей.

38. Таблица маршрутизации:
а) поддерживает широковещательные сообщения.
б) хранит адреса сетей.
в) предоставляет адрес ПК.

39. Отличие между мостами и маршрутизаторами:
а) мосты могут выбирать среди множества маршрутов.
б) мосты поддерживают среду Ethernet, но не поддерживают Token Ring.
в) маршрутизаторы могут выбирать среди множества маршрутов.

40. Устройство для обнаружения обрывов, коротких замыканий:
а) цифровой вольтметр.
б) рефлектометр.
в) тестеры.

Основная литература:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. - Москва : Издательство Юрайт, 2022. -333 с. -(Профессиональное образование). -ISBN 978-5-534-04638-0. -URL : https://urait.ru/bcode/491456
2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. -Москва : Издательство

Юрайт, 2022. -351 с. -(Профессиональное образование). -ISBN 978-5-534-04635-9. -URL : https://urait.ru/bcode/491951
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. -Москва : Издательство Юрайт, 2021. -312 с. -(Профессиональное образование). -ISBN 978-5-534-13221-2. -URL : https://urait.ru/bcode/476997

Дополнительная литература:

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. - Москва : Издательство Юрайт, 2021. -342 с. -(Профессиональное образование). -ISBN 978-5-534-10671-8. -Текст : электронный // Образовательная платформа Юрайт [сайт]. -URL: https://urait.ru/bcode/475889
2. Дибров М.В. Компьютерные сети и телекоммуникации. Маршрутизация в IP – сетях. В 2ч. Часть 1: учебник и практикум для СПО М.: Издательство Юрайт, 2020

Электронные источники:

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

КРИТЕРИИ ОЦЕНКИ
по дисциплине

МДК.01.03. СЕТИ И СИСТЕМА ПЕРЕДАЧИ ИНФОРМАЦИИ

Критерии оценки:

Оценка «отлично»: студент владеет знаниями предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивал при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи. Четко формирует ответы, решает ситуационные задачи повышенной сложности, хорошо знаком с основной литературой, увязывает теоретические аспекты предмета с задачами практического характера.

Оценка «хорошо»: студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах). Самостоятельно и отчасти при наводящих вопросах дает полноценные ответы, не всегда выделяет наиболее существенное, не допускает вместе с тем серьезных ошибок в ответах, умеет решать легкие и средней тяжести ситуационные задачи.

Оценка «удовлетворительно»: студент владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками. В процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.

Оценка «неудовлетворительно»: студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал, отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Вопросы к экзамену по дисциплине «Сети и система передачи информации»:

1. Виды сетей.
2. Основные составляющие сети.
3. Основные понятия и определения
4. Понятие протокола.
5. Иерархия протоколов.
6. Интерфейсы и сервисы.
7. Обобщенная структурная схема сети.
8. Методы коммутации информации в сетях связи
9. Основные технологии сетей передачи данных.
10. Стандартизирующие организации.
11. Общегосударственная система автоматической телефонной связи.
12. Построение городских и сельских телефонных сетей.
13. Архитектура и классификация телекоммуникационных сетей.
14. Особенности защищенных телекоммуникационных сетей.
15. Стандартизация телекоммуникационных сетей.
16. Стратегии межсетевого взаимодействия.
17. TCP/IP.
18. IPX/SPX
19. Среда передачи.
20. Коаксиальный кабель.
21. Витая пара.
22. Оптоволокно.
23. Структурированная кабельная система.
24. Активное сетевое оборудование.
25. Модуляция сигналов.
26. Амплитудная модуляция.
27. Частотная модуляция.
28. Фазовая модуляция.
29. Технология расширенного спектра
30. Кодирование сигнала.
31. Доступ к среде.
32. Группа стандартов.
33. Технология Ethernet.
34. Сети с маркерным доступом.
35. Технологии доступа с виртуальными каналами.
36. Технологии беспроводного доступа.
37. Технологии региональных сетей.
38. Основная концепция протоколов транспортного уровня.
39. Протокол TCP.
40. Формат пакета TCP.
41. Управление потоком.
42. Проблемы TCP. Протокол SCTP.

43.Формат пакета SCTP.
44.Множественность потоков и варианты доставки.
45.Протокол IPv4.
46.Формат пакета IP.
47.Схема адресации протокола IPv4.
48.Другие протоколы межсетевого уровня стека TCP/IP.
49.Протокол RARP.
50.Протокол ARP.
51.Протокол ICMP
52.Структурированная кабельная система.
53.Сетевые адаптеры.
54.Концентраторы.
55.Коммутаторы.
56.Мосты.
57.Шлюзы.
58.Маршрутизаторы.
59.Базовые технологии локальных сетей
60.Логическая структуризация сети.
61.Установка и конфигурирование сетевого оборудования.
62.Типовые схемы применения сетевого оборудования.
63.Беспроводные локальные сети.
64.Виртуальные локальные сети.
65.Потребность в применении VLAN.
66.Обобщенная структура и функции.
67.Назначение и структура сетей.
68.Интерфейсы глобальных сетей.
69.Сети выделенных каналов.
70.Сети с коммутацией каналов.
71.Сети с коммутацией пакетов.
72.Коммутация каналов.
73.Коммутация сообщений и пакетов
74.Технология ARPANET.
75.NSF.
76.Другие сетевые технологии
77.Организация удаленного доступа.
78.Обзор программного обеспечения.
79.Брандмауэры с фильтрацией пакетов.
80.Анализ сетевого трафика.
81.Фильтрация на прикладном уровне и другие защитные функции.
82.Защита сетевой ОС.
83.Настройка брандмауэра.
84.Установка и настройка FTP -сервера.
85.Доступ к серверу по протоколу FTP.
86.Создание учетных записей и групп пользователей.
87.Создание политик групп пользователей.

88. Установка и настройка DNS – сервера, DHCP-сервера и HTTP-сервера
89. Настройка брандмауэра.
90. Установка и настройка FTP -сервера.
91. Доступ к серверу по протоколу FTP.
92. Создание учетных записей и групп пользователей.
93. Создание политик групп пользователей.
94. Установка и настройка DNS – сервера, DHCP-сервера и HTTP-сервера
95. Техническая поддержка аппаратного обеспечения.
96. Техническая поддержка программного обеспечения.
97. Структурированная кабельная система.
98. Мероприятия по определению и обеспечению качественного состояния кабельных линий.
99. Определение технического состояния основных блоков сети.
100. Коэффициент для оценки технического состояния КС.

Правила выполнения практических работ:

При выполнении практических работ (ПР), студенты должны соблюдать и выполнять следующие правила:

11. Прежде, чем приступить к выполнению ПР, обучающийся должен подготовить ответы на теоретические вопросы к ПР.
12. Перед началом каждой работы проверяется готовность обучающегося к ПР.
13. После выполнения ПР студент должен представить отчет о проделанной работе в рабочей тетради или в собственном файле (в ПК) и подготовиться к обсуждению полученных результатов и выводов.
14. Студент (обучающийся), пропустивший выполнение ПР по уважительной или неуважительной причинам, обязан выполнить работу в дополнительно назначенное время.
15. Оценка за ПР выставляется с учетом предварительной подготовки к работе, доли самостоятельности при ее выполнении, точности и грамотности оформления отчета по работе.

Критерии оценки практических работ

Практические работы оцениваются по пятибалльной шкале.

Оценка «отлично»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, необходимые программы запущены и работают без ошибок; работа оформлена аккуратно;

Оценка «хорошо»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, частично с помощью преподавателя, присутствуют незначительные ошибки при запуске и эксплуатации (работе) необходимых программ; работа оформлена аккуратно;

Оценка «удовлетворительно»: частично с помощью преподавателя, присутствуют ошибки при запуске и работе требуемых программ; по оформлению работы имеются замечания.

Оценка «неудовлетворительно»: ставится, если обучающийся не подготовился к ПР, при запуске и эксплуатации (работе) требуемых программ студент допустил грубые ошибки, по оформлению работы имеются множественные замечания.

Тематика практических работ и задания к ним

1. Практическая работа 1. Построение одноранговой сети
2. Практическая работа 2. Определение MAC-адреса узла
3. Практическая работа 3. Определение IP-адреса компьютера
4. Практическая работа 4. IP-адресация и обмен данными в сети

Практическая работа 1. Построение одноранговой сети

Задачи

- Спроектировать и построить простую одноранговую сеть с помощью перекрестного кабеля, предоставленного преподавателем.
- Проверить соединение между равноправными узлами с помощью команды ping.

Исходные данные / подготовка

На этой практической лабораторной работе требуется спроектировать и построить простую одноранговую сеть с помощью двух ПК и перекрестного кабеля Ethernet.

Требуются следующие ресурсы:

- два ПК с Windows XP Professional, на каждом из которых установлена и функционирует сетевая интерфейсная плата;
- перекрстный кабель Ethernet.

Шаг 1. Составление схемы сети

а) Схема сети – это карта логической топологии сети. На представленном ниже пустом пространстве начертите простую одноранговую сеть,

связывающую два ПК. Один ПК пометьте IP-адресом 192.168.1.1, а второй ПК – IP-адресом 192.168.1.2. Пометьте все соединители и необходимые сетевые устройства.

б) В простой сети, подобной той, что проектируется, может использоваться концентратор или коммутатор в качестве центрального устройства связи, либо же ПК могут быть связаны напрямую. Какой тип кабеля требуется для прямого Ethernet-соединения двух
ПК?

Шаг 2. Документирование ПК

а) Проверьте параметры имени компьютера для каждого ПК и измените их при необходимости. На каждом ПК нажмите кнопку «Пуск» и выберите пункт «Панель управления». Дважды щелкните значок «Система», а затем перейдите на вкладку «Имя компьютера». Запишите имя компьютера, которое отображается после записи «Полное имя:».
Имя компьютера PC1:
Имя компьютера PC2:

б) Проверьте, не обладают ли оба ПК одним именем. Если это так, измените имя одного из ПК, нажав кнопку «Изменить», введя новое имя в поле «Имя компьютера», а затем нажмите кнопку «ОК».

в) Нажмите кнопку «ОК», чтобы закрыть окно «Свойства системы».

г) Почему так важно, чтобы все ПК в сети обладали уникальным именем?

Шаг 3. Подключение кабеля Ethernet

а) Используйте перекрестный кабель Ethernet, предоставленный преподавателем. Вставьте один конец кабеля в сетевую плату Ethernet компьютера PC1.

б) Другой конец кабеля вставьте в сетевую плату Ethernet компьютера PC2. При подключении конца кабеля должен быть слышен щелчок, указывающий на то, что кабель вставлен в порт правильно.

Шаг 4. Проверка физического соединения

а) После подключения перекрестного кабеля Ethernet к обоим ПК, внимательно осмотрите каждый порт Ethernet. Световая индикация (обычно зеленого или желтого цвета) означает, что между двумя сетевыми платами установлено физическое соединение. Попробуйте отключить кабель от одного из ПК, а затем снова подключить, чтобы проверить, как световая индикация отключается и снова включается.

б) Перейдите в «Панель управления», дважды щелкните значок «Сетевые подключения» и убедитесь, что подключение по локальной сети установлено. На следующем рисункепоказан пример активного подключения по локальной сети. При наличии неполадок физического подключения на значке «Подключение по локальной сети» виден знак X и сообщение «Сетевой кабель не подключен».

в) Если в значке «Подключение по локальной сети» не указывается, что соединение установлено, устраните неполадки, повторив шаги 3 и 4. Можно также попросить преподавателя подтвердить, что используется перекрестный кабель Ethernet.

Шаг 5. Настройка параметров IP

а) Настройте логические адреса двух ПК, чтобы они могли связываться по протоколу TCP/IP. На одном ПК перейдите в панель управления, дважды щелкните значок «Сетевые подключения» и правой кнопкой мыши щелкните значок установленного подключения по локальной сети. В раскрывающемся меню выберите пункт «Свойства».
б) С помощью полосы прокрутки в окне «Подключение по локальной сети – свойства», прокрутите список до элемента «Протокол Интернета (TCP/IP)». Нажмите кнопку «Свойства».
в) Установите переключатель «Использовать следующий IP-адрес» и введите следующую информацию: IP-адрес 192.168.1.1 Маска подсети 255.255.255.0
г) Нажмите кнопку «ОК», чтобы закрыть окно «Свойства: Протокол Интернета (TCP/IP)». Нажмите кнопку «Закрыть», чтобы закрыть окно «Подключение по локальной сети – свойства».
д) Повторите шаги 5a – 5d на втором ПК, используя следующую информацию: IP-адрес 192.168.1.2 Маска подсети 255.255.255.0

Шаг 6. Проверка IP-соединения между двумя ПК

ПРИМЕЧАНИЕ. Для проверки соединения TCP/IP на обоих ПК необходимо временно отключить брандмауэр Windows. После завершения проверки межсетевой экран Windows следует снова включить.

а) На рабочем столе Windows XP компьютера PC1 нажмите кнопку «Пуск». В меню «Пуск» выберите пункт «Панель управления» и дважды щелкните значок «Сетевые подключения».
б) Правой кнопкой мыши щелкните значок «Подключение по локальной сети» и выберите пункт «Свойства». Перейдите на вкладку «Дополнительно». Найдите и нажмите кнопку «Параметры».
в) Проверьте, какие у межсетевой экран настройки: «ВКЛЮЧЕН (ВКЛ.) для порта Ethernet» или «ВЫКЛЮЧЕН (ВЫКЛ.) для порта Ethernet». г. Если брандмауэр включен, установите переключатель «Выключить (не рекомендуется)», чтобы отключить межсетевой экран. В дальнейшем межсетевой экран будет снова включен. Нажмите кнопку «ОК» в данном диалоговом окне и в следующем, чтобы применить изменения.
г) Теперь, когда два ПК физически соединены и в них правильно настроены IP-адреса, необходимо убедиться в их способности связываться друг с

другом. Команда ping – самый простой способ выполнения этой задачи. Команда ping включена в операционную систему Windows XP:

д) На компьютере PC1 нажмите кнопку «Пуск», а затем выберите команду «Выполнить». Введите команду cmd, а затем нажмите кнопку «ОК». Откроется окно командной строки Windows (см. рисунок ниже). 10
е) В командной строке > введите ping 192.168.1.2 и нажмите клавишу ВВОД. Успешное выполнение команды ping подтверждает IP-подключение. Пример выходных данных представлен ниже.
ж) Повторите шаги 6а-6с на втором ПК. На втором ПК требуется выполнить команду ping 192.168.1.1. и. Закройте окно командной строки Windows на обоих ПК.

Шаг 7. Проверка соединения с помощью компонента «Сетевое окружение»

а) Любой ПК может открывать свои ресурсы для совместного использования другими ПК в сети. Доступ к списку ПК с общими ресурсами можно получить с помощью компонента «Сетевое окружение». На компьютере PC1 нажмите кнопку «Пуск», выберите пункт «Сетевое окружение», а затем в левой панели щелкните ссылку «Отобразить компьютеры рабочей группы».
б) Виден ли значок другого ПК в локальной одноранговой сети?
в) Какое имя у другого ПК?
г) Это имя, записанное на шаге 2?
д) Повторите шаг 7а на втором ПК.
е) Закройте все открытые окна.

Шаг 8. Повторное включение межсетевого экрана (необязательный – используется, только если изначально межсетевой экран был ВКЛЮЧЕН)

а) Если на шаге 6 межсетевой экран Windows был отключен, нажмите кнопку «Пуск», выберите «Панель управления», а затем откройте ее компонент «Сетевые подключения».
б) Правой кнопкой мыши щелкните значок «Подключение по сети Ethernet» и выберите пункт «Свойства». Перейдите на вкладку «Дополнительно». Найдите и нажмите кнопку «Параметры».

   Если межсетевой экран отключен (но был включен перед началом лабораторной работы), установите переключатель «Включить (рекомендуется)», чтобы включить межсетевой экран. Нажмите кнопку «ОК» в данном диалоговом окне и в следующем, чтобы применить изменения.

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений) по дисциплине «Сети и система передачи информации»:

1. Направления развития аппаратно-программных методов и средств сетевого контроля и диагностики сетей ЭВМ.
2. Направления развития аппаратно-программных методов и средств сетевого контроля и диагностики локальных вычислительных сетей (ЛВС).
3. Коммутаторы в сетях ЭВМ. Сравнительный анализ и пути развития.
4. Маршрутизаторы в сетях ЭВМ. Сравнительный анализ и пути развития.
5. АТМ - технология. Сравнительный анализ. Способы и средства реализации. Области рационального применения.
6. Глобальные и локальные сети ЭВМ. Сравнительный анализ. Способы интеграции и взаимодействия. Области использования.
7. Аппаратно-программные средства доступа в сети ЭВМ. Сравнительный анализ. Варианты построения и реализации, области применения.

8. Серверы в сетях ЭВМ. Типы, характеристики, области применения.
9. Сетевые протоколы в сетях ЭВМ. Сравнительный анализ. Тенденции развития. Средства реализации.
10. Средства и протоколы управления в сетях ЭВМ, Сравнительный анализ. Тенденции развития. Способы реализации.
11. Защита ЛВС и информации в ЛВС. Способы и средства защиты. Направления
развития средств защиты.
12. Сетевые архитектуры ЛВС. Виды. Сравнительный анализ. Области применения.
13. Сетевые архитектуры систем передачи данных. Виды, сравнительный анализ. Тенденции развития.
14. Терминальные (абонентские) комплексы сетей ЭВМ. Сравнительный анализ. Способы построения. Тенденции развития.
15. Эволюция сетей связи с коммутацией каналов.
16. Эволюция сетей связи с коммутацией пакетов.
17. Эволюция WWW.
18. Эталонная модель OSI/ISO.
19. Эталонная модель TCP/IP.
20. Цифровые сети с интеграцией служб ISDN.
21. Режим асинхронной передачи ATM.
22. Сети подвижной связи GSM.
23. Сети подвижной связи GSM/GPRS.
24. Сети подвижной связи CDMA.
25. Беспроводные сети Wi-Fi.
26. Беспроводные сети WiMax.
27. Протоколы множественного доступа, система ALOHA.14. Протоколы множественного доступа, стандарт Ethernet.
28. Сетевой уровень, алгоритмы маршрутизации.
29. Сетевой уровень, алгоритмы управления перегрузками.
30. Протокол OSPF.
31. Протокол BGP.
32. Протоколы мультивещания.
33. Технология коммутации по меткам MPLS.
34. Протокол TCP.
35. Протокол SCTP.
36. Система сигнализации №7, технология Sigtran.
37. Протокол http.
38. Служба доменных имен DNS.
39. Архитектура WWW.
40. Сеть управления TMN.

СТРУКТУРА ИТОГОВОГО ТЕСТА:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Сети и системы передачи информации»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	Оценка знаний
90-100	5 «отлично»

75-89	4 «хорошо»
60-74	3 «удовлетворительно»
Менее 60	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ) по дисциплине «Сети и система передачи информации»

1. Какой уровень модели OSI является высшим:
   а) сеансовый
   б) представительский
   в) прикладной
2. На каком уровне Модели OSI строится таблица маршрутизации:
   а) транспортный
   б) сеансовый
   в) сетевой
3. Сколько уровней включает в себя эталонная модель OSI:
   а) 7
   б) 9
   в) 5
4. В какой сетевой топологии необходим центральный узел:
   а) звезда
   б) шина
   в) кольцо
5. Для чего используется технология попарно свитых проводников:
   а) уменьшение перекрестных наводок
   б) уменьшение коэффициента затухания
   в) уменьшения волнового сопротивления
6. В каких сетях применяется экранированная витая пара:
   а) FDDI
   б) Frame Relay
   в) Toktn Ring
7. Какой диаметр имеет сердечник многомодового волоконно-оптического кабель:
   а) 40 мкм
   б) 60 мкм
   в) 80 мкм
8. Какое максимальное расстояние между двумя узлами при использовании одномодового волоконно-оптического кабеля:
   а) 40 км
   б) 60 км
   в) 100 км
9. Какой размер кадра при коммутации ячеек:

а) 32
б) 53
в) 64

10. Как называется канал связи существующий некоторое время:
    а) сеансовый
    б) выделенный
    в) коммутируемый
11. При каком способе коммутации данные разбиваются на блоки фиксированной длины:
    а) коммутации каналов
    б) коммутации сообщений
    в) коммутации пакетов
12. При каком способе коммутации канал связи немонополизируется :
    а) коммутация каналов
    б) коммутация сообщений
    в) коммутация пакетов
13. Какая сетевая технология использует коммутацию ячеек:
    а) АТМ
    б) АРМ
    в) АНМ
14. Какое сетевое устройство оперирует сетевыми адресами:
    а) мост
    б) маршрутизатор
    в) коммутатор
15. Какой из видов мостов не использует «конверты»:
    а) инкапсулирующие
    б) прозрачные
    в) транслирующие
16. Какое сетевое устройство работает с учетом метрики:
    а) мосты
    б) маршрутизаторы
    в) коммутаторы
17. Какие маршрутизаторы характеризуются низкой стоимостью:
    а) периферийные
    б) удаленного доступа
    в) магистральные
18. Какой самый распространенный стек протоколов:
    а) IPX
    б) XNS
    в) TCP/IP
19. Какой стек протоколов наиболее приближен к модели OSI:
    а) DECnet
    б) AplleTalk
    в) SNA
20. На каком уровне стека протоколов TCP/IP решаются задачи надежности:

а) сетевой интерфейс
б) межсетевой
в) транспортный

21. Какой протокол прикладного уровня:
а) TCP
б) DNS
в) ARP

22. Какой протокол оперирует дейтаграммами:
а) RIP
б) UTP
в) TCP

23. Какая программа позволяет перехватывать сетевой трафик:
а) сниффер
б) риффер
в) глиффер

24. В каком протоколе информация между клиентом и сервером передается открытым текстом:
а) HTTP
б) DNS
в) DHCP

25. Физический адрес:
а) PAC
б) BAC
в) MAC

26. Протокол установления сеанса:
а) DIP
б) RIP
в) SIP

27. Протокол передачи почты:
а) SMTP
б) SNMP
в) TFTP

28. Протокол передачи гипертекста:
а) DHCP
б) HTTP
в) SMTP

29. Виртуальный текстовый терминал:
а) TELnet
б) SELnet
в) WELnet

30. Туннельный протокол типа точка-точка:
а) PPRP
б) RPPT
в) PPTP

Основная литература:

1. *Дибров, М. В.* Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. - Москва : Издательство Юрайт, 2022. - 333 с. - (Профессиональное образование). - ISBN 978-5-534-04638-0. - URL : https://urait.ru/bcode/491456
2. *Дибров, М. В.* Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. - Москва : Издательство Юрайт, 2022. - 351 с. - (Профессиональное образование). - ISBN 978-5-534-04635-9. - URL : https://urait.ru/bcode/491951
3. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва : Издательство Юрайт, 2021. - 312 с. - (Профессиональное образование). - ISBN 978-5-534-13221-2. - URL : https://urait.ru/bcode/476997
4. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - Москва : Издательство Юрайт, 2022. - 363 с. - (Профессиональное образование). - ISBN 978-5-9916-0480-2. - URL : https://urait.ru/bcode/495353

Дополнительная литература:

1. Берикашвили, В. Ш. Основы радиоэлектроники: системы передачи информации: учебное пособие для среднего профессионального образования / В. Ш. Берикашвили. - 2-е изд., испр. и доп. - Москва: Издательство Юрайт, 2019. - 105 с. - (Профессиональное образование). - ISBN 978-5-534-10493-6. - Текст: электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/430609.
2. Велихов А.В. Компьютерные сети. – М.: Познавательная книга пресс, 2012. -319с.
3. Велихов А.В. Компьютерные сети. Учебное пособие по администрированию локальных и объединенных сетей. - Спб.: Питер, 2013. - 304с.

Интернет-ресурсы:

1. Библиотека Альдебаран – компьютерная литература [Электронный ресурс]. – Режим доступа: http://www.aldebarans.ru/komp, свободный. – Загл. с экрана.
2. Википедия – Свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org, свободный. – Загл. с экрана.

3. Официальный сайт Министерства образования и науки Российской Федерации. – Режим доступа: http://www.mon.gov.ru, свободный. – Загл. с экрана.
4. Педагогика.ру – Справочный сайт [Электронный ресурс]. – Режим доступа: http://www.pedagogy.ru, свободный. – Загл. с экрана.
5. Портал нормативно-технической документации [Электронный ресурс]. – Режим доступа: http://www.pntdoc.ru, свободный. – Загл. с экрана.
6. Российское образование. Федеральный портал [Электронный ресурс].. – Режим доступа: http://www.edu.ru, свободный. – Загл. с экрана.
7. Техническая литература [Электронный ресурс]. – Режим доступа: http://www.tehlit.ru, свободный. – Загл. с экрана

КРИТЕРИИ ОЦЕНКИ
по дисциплине

МДК.01.04. АНТИВИРУСНАЯ СИСТЕМА

Критерии оценки:

Оценка «отлично»: студент владеет знаниями предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивал при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи. Четко формирует ответы, решает ситуационные задачи повышенной сложности, хорошо знаком с основной литературой, увязывает теоретические аспекты предмета с задачами практического характера.

Оценка «хорошо»: студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах). Самостоятельно и отчасти при наводящих вопросах дает полноценные ответы, не всегда выделяет наиболее существенное, не допускает вместе с тем серьезных ошибок в ответах, умеет решать легкие и средней тяжести ситуационные задачи.

Оценка «удовлетворительно»: студент владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками. В процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.

Оценка «неудовлетворительно»: студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал, отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Вопросы к дифференцированному зачету по дисциплине «Антивирусная система»:

1. Типы вредоносных программ.
2. Общее определение компьютерного вируса
3. Различные типы вирусов
4. Файловые вирусы
5. Загрузочные вирусы
6. Файлово-загрузочные вирусы
7. Стелс-вирусы
8. Шифрующиеся вирусы
9. Полиморфные вирусы
10. Макрокомандные вирусы
11. Почтовые вирусы
12. Вирусы в пакетных файлах ОС
13. Вирусы в драйверах ОС
14. Бестелесные вирусы
15. Вирусы для пиринговых сетей
16. Комбинированные вирусы
17. Известные и неизвестные вирусы
18. Коллекционные вирусы
19. Логические бомбы
20. Троянские объекты
21. Троянские программы
22. Троянские Web-сайты
23. Троянские сообщения E-Mail
24. Программы Backdoor
25. Средства для получения несанкционированного доступа
26. Техника Phishing
27. Программы Spyware
28. Программы Adware
29. Клавиатурный шпион
30. Комбинированные вредоносные программы
31. Файлы исполняемых программ
32. Файлы офисных документов
33. Файлы интерпретируемых программ
34. Загрузочные секторы дисков и дискет
35. Сообщения электронной почты
36. Файлообменные (пиринговые) сети
37. Визуальные и звуковые эффекты
38. Воздействие на файлы
39. Изменение содержимого секторов диска
40. Воздействие на базы данных
41. Воздействие на аппаратное обеспечение компьютеров
42. Воздействие на систему в целом

43. Получение несанкционированного доступа и похищении информации
44. Компрометация пользователя
45. Социальный инжиниринг
46. Сканирование. Эвристический анализ. Обнаружение изменений
47. Анализ сетевого трафика. Анализ баз данных почтовых программ
48. Обнаружение вирусов в системе автоматизации документооборота
49. Вакцинирование
50. Сканеры. Сканирование по запросу пользователя. Сканирование при обращении к файлам. Сканирование по расписанию. Сканирование сетевого трафика
51. Ревизоры диска
52. Встроенные антивирусы
53. Программа Kaspersky Anti-Virus
54. Программа Dr.Web
55. Программа Norton Antivirus
56. Прочие антивирусные программы
57. Программа Stop!
58. Программа Panda Antivirus
59. Программа Virus Scan
60. Проблемы защиты крупных корпоративных интрасетей
61. Функции удаленного управления и контроля
62. Удаленное обновление антивирусных баз данных
63. Децентрализованная установка и обновление антивирусов с сетевым центром управления
64. Удаленная настройка антивирусных программ. Обнаружение новых рабочих станций. Планирование заданий
65. Сигнальное информирование. Архитектура и принципы работы корпоративных систем антивирусной защиты. Состав дистрибутива
66. Сканер Dr.Web. Сторож SpIDer Guard
67. Почтовый сторож SpIDer Mail. Планировщик заданий
68. Утилита обновления. Процедура установки пакета Dr.Web для Windows
69. Удаление пакета Dr.Web для Windows
70. Стандартный пакет Dr.Web для Windows и пакет Dr.Web Home Edition
71. Параметры проверки объектов. Принципы отбора файлов для сканирования. Состав дистрибутива пакета ESET Nod32/Ср/
72. Установка и удаление пакета ESET Nod32/Ср/ . Требования к установленным программам
73. Требования к конфигурации компьютера
74. Особенности пакета ESET Nod32/Ср/. Конфигурация пакета ESET Nod32/Ср/. Удаление пакета ESET Nod32/Ср/
75. Ознакомительная версия пакета Dr.Web для Unix. Установка файла регистрационного ключа. Обновление пакета ESET Nod32/Ср/ для Unix
76. Вирусные базы данных пакета ESET Nod32/Ср/ для Unix
77. Состав дистрибутива. Установка пакета Sophos Small Business Suite. Первый этап установки. Второй этап установки. Установка вручную

78. Установка на компьютеры, не подключенные к Интернету. Просмотр состояния антивирусной защиты на узлах сети. Добавление новых компьютеров
79. Обновление антивирусов и антивирусной базы данных. Проверка файлов в автоматическом режиме
80. Состав дистрибутива. Установка и настройка. Требования к операционной системе. Требования к установленным программам. Требование к квалификации пользователя.
81. Процесс установки. Конфигурация Kaspersky 6.0 для Windows. Параметры проверки объектов.

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений) по дисциплине «Антивирусная система»:

1. Основные понятия информационной безопасности
2. Угрозы безопасности информации, их классификация

3. Криптографические методы информационной безопасности
4. Нормативно-правовое обеспечение информационной безопасности
5. Организационные методы защиты информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации КС для обеспечения заданного уровня безопасности информации
6. Программные средства борьбы с вирусами.
7. Оценка рисков информационных угроз безопасности
8. Профилактика заражения вирусами компьютерных систем
9. Антивирусная защита компьютерных систем
10. Хронология возникновения вирусов
11. Понятие «Компьютерный вирус»
12. Авторы компьютерных вирусов
13. История компьютерных вирусов
14. Механизм работы вирусов
15. Способы распространения компьютерных вирусов
16. Признаки заражения вирусом
17. Лицензионные антивирусные программы
18. Альтернатива платным программам

СТРУКТУРА ИТОГОВОГО ТЕСТА:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Антивирусные системы»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	Оценка знаний
90-100	5 «отлично»
75-89	4 «хорошо»
60-74	3 «удовлетворительно»
Менее 60	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ) по дисциплине «Антивирусная система»

1. Что такое "компьютерный вирус"?
    а) это программы, активизация которых вызывает уничтожение программ и файлов
    б) это совокупность программ, находящиеся на устройствах долговременной памяти
    в) это программы, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы
    г) это программы, передающиеся по Всемирной паутине в процессе загрузки Web-страниц
2. К каким вирусам относится "троянский конь"?
    а) макро-вирусы

б) интернет-черви
в) скрипт-вирусы
г) загрузочные вирусы

3. Какие файлы заражают макро-вирусы?
   а) исполнительные;
   б) графические и звуковые;
   в) файлы документов Word и электронных таблиц Excel;
   г) html документы
4. Если есть признаки заражения вирусом, нужно:
   а) проверить диск антивирусной программой
   б) отформатировать диск
   в) пригласить специалиста, чтобы изучить и обезвредить вирус
   г) скопировать свои файлы на внешний носитель и перейти работать на другой компьютер
5. К биометрической системе защиты относится:
   а) защита паролем
   б) идентификация по радужной оболочке глаз
   в) антивирусная защита
   г) физическая защита данных
6. Программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации…
   а) межсетевой экран;
   б) иммунизатор;
   в) антивирусная программа;
   г) CRC-сканер.
7. Основные угрозы доступности информации:
   а) непреднамеренные ошибки пользователей
   б) злонамеренное изменение данных
   в) хакерская атака
   г) перехват данных
8. Сервисы безопасности:
   а) кэширование записей
   б) идентификация и аутентификация
   в) инверсия паролей
   г) регулирование конфликтов
9. К формам защиты информации не относится…
   а) аналитическая
   б) правовая
   в) организационно-техническая
   г) биометрическая
10. Что не является базовым принципом информационной безопасности:
   а) целостность данных
   б) конфиденциальность информации

в) доступ к информации для авторизированных пользователей
г) короткий, легко запоминающийся пароль

11. Несанкционированным доступом является
а) недостаточное знание работниками предприятия правил защиты информации
б) слабый контроль за соблюдением правил защиты информации
в) хищение носителей информации и документальных отходов

12. Реализации угроз информационной безопасности способствуют
а) болтливость
б) простудные заболевания
в) Налоговый кодек.

13. Типовыми путями несанкционированного доступа к информации, являются:
а) дистанционное фотографирование;
б) выход из строя ПЭВМ;
в) ураганы.

14. Угрозы доступности данных возникают в том случае, когда?
а) объект не получает доступа к законно выделенным ему ресурсам
б) легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность
в) случаются стихийные бедствия.

15. Внедрение компьютерных вирусов является следующим способом воздействия угроз на информационные объекты?
а) информационным;
б) физическим;
в) программно-математическим способом.

16. Логическая бомба – это?
а) компьютерный вирус
б) способ ведения информационной войны
в) прием, используемый в споре на философскую тему

17. Объектом информационной атаки не является:
а) АИС в целом;
б) каналы передачи данных;
в) природоохранные мероприятия.

18. Под «маскарадом» понимается?
а) выполнение каких-либо действий одним пользователем от имени другого пользователя;
б) обработка денежных счетов при получении дробных сумм;
в) монополизация какого-либо ресурса системы.

19. «Люком» называется?
а) использование после окончания работы части данных, оставшиеся в памяти
б) передача сообщений в сети от имени другого пользователя

в) не описанная в документации на программный продукт возможность работы с ним

20. «Мобильные» вирусы распространяются:
    а) путем взлома программ ВЭВМ
    б) в виде «червей» и «троянцев» для мобильных телефонов
    в) по линии связи между узлами сети

Основная литература:

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. - Москва : Издательство Юрайт, 2018. - 321 с. - (Университеты России). - ISBN 978-5-534-00258-4. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/414248
2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. - Москва : Издательство Юрайт, 2021. - 253 с. - (Высшее образование). - ISBN 978-5-534-13960-0. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/467370
3. Мельников, Куприянов: Информационная безопасность (для СПО). Учебник. Подробнее: https://www.labirint.ru/books/632515/
4. https://frolov-lib.ru/books/av/ch19.html

Дополнительная литература:

1. Белов Е.Б. Основы информационной безопасности: Учебн. пособие/
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. - М.: Горячая линия - Телеком.
3. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебн. пособие / Бузов Г.А., Калинин С.В., Кондратьев А.В.- М.: Горячая линия - Телеком, 2005. - 416 с.
4. Запечников С.В. Информационная безопасность открытых систем. Часть 1: Учебник для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И.,
5. Ушаков Д.В. - М.: Горячая линия - Телеком, 2006. - 686 с.
6. Малюк А.А. Введение в защиту информации в автоматизированны системах: Учебн. пособие для вузов / Малюк А.А., Пазизин С.В., Погожий Н.С. - М.: Горячая линия - Телеком, 2004. - 147 с.
7. Снытников А.А. Лицензирование и сертификация в области защиты информации. - М.: Гелиос АРВ, 2003. - 192 с.
8. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005.-304 с.
9. Хорев А.А. Защита информации от утечки по техническим каналам: Учебн. пособие. - М.: МО РФ, 2006.

10. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на-Дону: Издательство СКНЦ ВШ, 2006.

Интернет-ресурсы:

1. Библиотека Альдебаран – компьютерная литература [Электронный ресурс]. – Режим доступа: http://www.aldebarans.ru/komp, свободный. – Загл. с экрана.
2. Википедия – Свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org, свободный. – Загл. с экрана.
3. Официальный сайт Министерства образования и науки Российской Федерации. – Режим доступа: http://www.mon.gov.ru, свободный. – Загл. с экрана.
4. Педагогика.ру – Справочный сайт [Электронный ресурс]. – Режим доступа: http://www.pedagogy.ru, свободный. – Загл. с экрана.
5. Портал нормативно-технической документации [Электронный ресурс]. – Режим доступа: http://www.pntdoc.ru, свободный. – Загл. с экрана.
6. Российское образование. Федеральный портал [Электронный ресурс].. – Режим доступа: http://www.edu.ru, свободный. – Загл. с экрана.
7. Техническая литература [Электронный ресурс]. – Режим доступа: http://www.tehlit.ru, свободный. – Загл. с экрана