

Документ подписан простой электронной подписью  
 Информация о владельце:  
 ФИО: Космож Сергей Михайлович  
 Должность: ректор  
 Дата подписания: 18.06.2025 14:12:36  
 Уникальный идентификатор документа:  
 e3a68f33e2d1c62674154f499808917c6bfdfc836

## Оценочные материалы для промежуточной аттестации по дисциплине

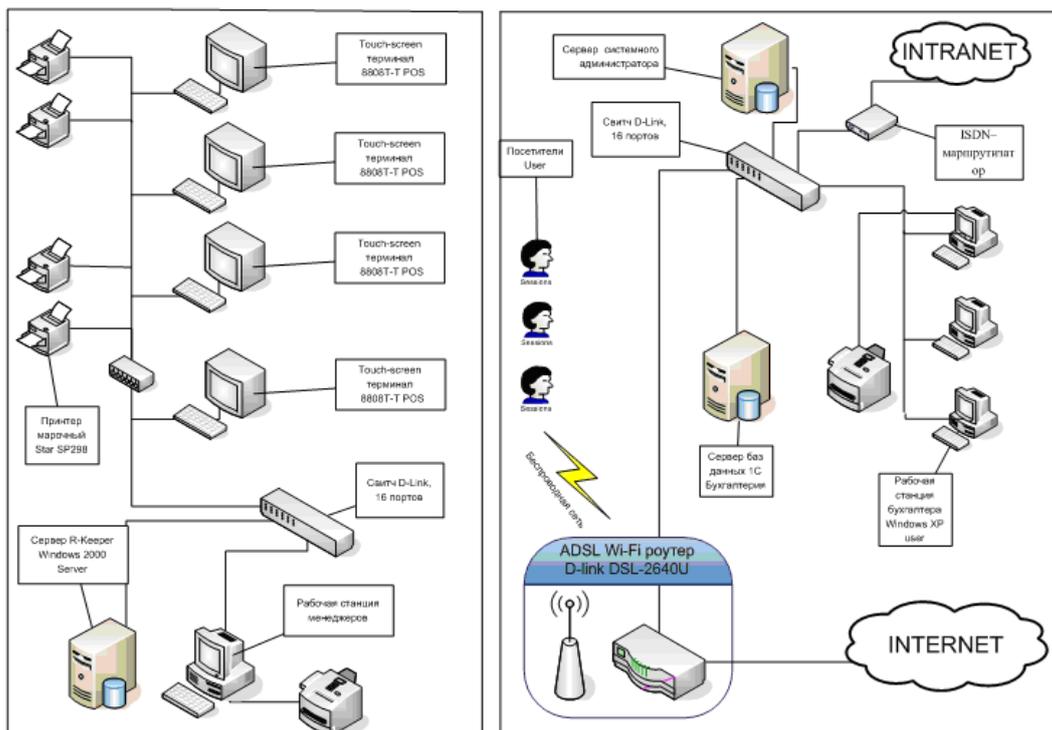
### Информационная безопасность систем связи и телекоммуникаций, 8 семестр

Код, направление	11.03.02 Инфокоммуникационные технологии и системы связи
подготовки	Корпоративные инфокоммуникационные системы и сети
Направленность (профиль)	Очная
Форма обучения	Радиоэлектроники и электроэнергетики
Кафедра-разработчик	Радиоэлектроники и электроэнергетики
Выпускающая кафедра	Радиоэлектроники и электроэнергетики

Задание для контрольной работы:

1. Тема контрольной работы «Разработка системы обеспечения информационной безопасности корпоративных сетей».
2. Цель – разработки системы обеспечения информационной безопасности корпоративной сети предприятия.
3. Задание.

Задана схема корпоративной сети предприятия.



Требуется:

- 1) Выбрать трассу и обосновать проектные решения.
- 2) Разработать оптимальную структуру сети.
- 3) Обеспечить сетевую устойчивость.
- 4) Рассчитать параметры линии передачи.
- 5) Разработать компьютерную модель оценки показателей структурной надежности телекоммуникационной сети.

- 6) Рассчитать показатели структурной надежности телекоммуникационной сети по компьютерной модели.
- 7) Определить требования к информационной безопасности корпоративной сети со стороны пользователей.
- 8) Определить методы аутентификации и криптографической защиты.
- 9) Определить состав элементов системы информационной безопасности корпоративной сети.
- 10) Разработать план развертывания системы обеспечения информационной безопасности корпоративной сети.
- 11) Разработать порядок настройки элементов системы информационной безопасности корпоративной сети.

4. Период выполнения: в период подготовки к экзамену с 3 недели до дня проведения экзамена. Контрольная работа сдается преподавателю для проверки не позднее, чем за день до экзамена. В период проведения экзамена проводится процедура оценивания контрольной работы. Результаты контрольной работы учитываются в итоговой оценке на экзамене.

Вопросы к экзамену:

1. Какие Вы знаете количественные характеристики надежности?
2. Какие Вы знаете количественные характеристики восстановления?
3. Какие Вы знаете характеристики потока отказов и восстановлений?
4. Какие Вы знаете характеристики готовности?
5. Модели отказов.
6. Модели восстановлений.
7. Как определяется надежность РТС без резервирования.
8. РТС с резервированием (горячий резерв).
9. Надежность РТС с резервированием последовательно соединенных блоков.
10. Надежность РТС с горячим резервом при замещении.
11. Скользящее резервирование.
12. Определение затрат на резервирование.
13. Граф состояний РТС с отказами и восстановлением.
14. Граф состояний РТС с отказами и очередью на восстановление (холодный резерв).
15. Граф РТС с поглощающим состоянием.
16. Задачи апостериорного анализа.
17. Оценка среднего времени безотказной работы.
18. Достоверность оценки среднего времени безотказной работы.
19. Доверительный интервал среднего времени безотказной работы.
20. Длительность испытаний.
21. Оценка среднего времени безотказной работы (процедура  $[n, V, r]$ ).
22. Проверка соответствия характеристик надежности техническим условиям.
23. Последовательная (пошаговая) процедура проверки гипотез.
24. Оценка закона распределения.
25. Назовите параметры для определения надежности сложных объектов согласно нормативной документации. Приведите примеры расчета выбранных параметров.

26. Перечислите характеристики и параметры оцениваемой модели. Приведите алгоритм расчета матрицы интенсивностей и матрицы вероятностей прохождений. Цель и последовательность решения обратной задачи.
27. Ошибки диагностирования и их влияние на рациональную периодичность технического обслуживания средств телекоммуникаций.
28. Критерии определения рациональной периодичности технического обслуживания средств телекоммуникаций. Адекватность математической модели исследуемым процессам.
29. Классификация методов определения надежности.
30. Статистические методы оценки показателей надежности. Краткая характеристика, примеры реализации.
31. Алгоритм расчета значений для оценки среднего времени восстановления и оценки вероятностей работоспособного и неработоспособного состояния объекта (системы).
32. Оценка интенсивности событий для случая полностью и неполностью определенной выборки. Алгоритм расчета.
33. Пояснить алгоритм решения задач сетевого анализа и синтеза.
34. Метод наискорейшего градиентного спуска, область применения, достоинства и недостатки.
35. Асимптотический подход к интервальному оцениванию (общий случай). Алгоритм нахождения интервальной оценки математического ожидания при известной дисперсии.
36. Поясните на примере алгоритм расчета математического ожидания числа связей. Что такое связность сети?
37. Аналитический и статистический методы расчета структурной надежности сети. Алгоритмы расчета, условия и возможности применения.
38. Методы повышения структурной надежности телекоммуникационных сетей.
39. Поясните на примере алгоритм нахождения кратчайшего пути (алгоритм Дейкстры).
40. Условия, определяющие характер функционирования телекоммуникационных систем.
41. Объекты защиты информации в телекоммуникационных системах.
42. Анализ основных закономерностей.
43. Анализ угроз безопасности информации в телекоммуникационных системах.
44. Анализ закономерностей функционирования телекоммуникационных систем.
45. Анализ закономерностей функционирования компонентов телекоммуникационных систем, обуславливающих угрозы безопасности информации.
46. Особенности сигналов, обрабатываемых на объектах телекоммуникационных систем.
47. Проблема разграничения доступа и защиты от несанкционированного доступа.
48. Проблема обеспечения информационной безопасности в территориально распределенной системе.
49. Проблема обеспечения безопасности информации при реализации нетрадиционных для ТКС ОГУ видов информационных услуг.
50. Проблема специальных исследований на предмет наличия аппаратных и программных закладок.

51. Проблема интегральной оценки защищенности информации при использовании различных средств комплексной защиты информации.
52. Проблема разведзащищенности системы (защиты от демаскирования).
53. Проблема комплексной защиты информации по всем компонентам ТКС ОГУ.
54. Проблема ЗИ при выходе на международные сети, подключении пользователей (абонентов) негосударственных структур.
55. Проблема разработки оптимальных ключевых структур.
56. Проблема организации управления защитой информации.
57. Проблема построения защищенной системы на основе принципиально открытой модели.
58. Проблема аутентификации абонентов и абонентских установок.
59. Проблема защиты от преднамеренной перегрузки ресурсов системы и переадресации информации.
60. Обоснование структуры системы комплексного контроля безопасности информации.