Оценочные материалы для промежуточной аттестации по дисциплине

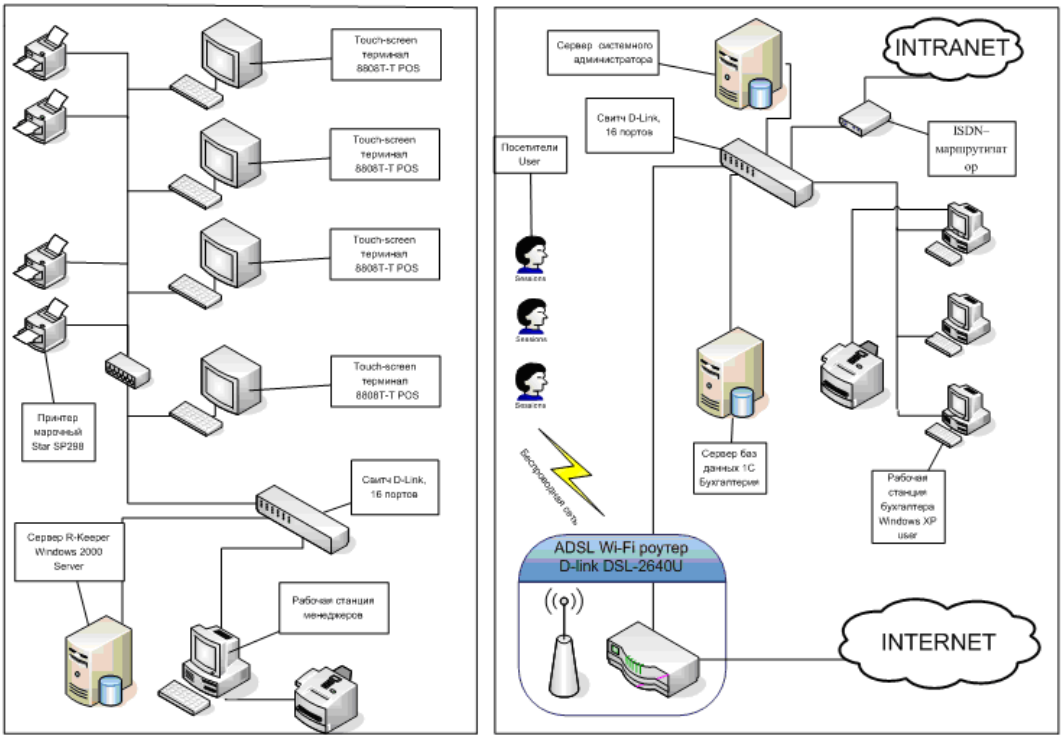
Безопасность корпоративных сетей, 3 семестр

Код, направление подготовки	11.04.02. Инфокоммуникационные технологии и системы связи
Направленность (профиль)	Корпоративные инфокоммуникационные системы и сети
Форма обучения	Очная
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) Определить требования к информационной безопасности корпоративной сети со стороны пользователей.
2) Определить методы аутентификации и криптографической защиты.
3) Определить состав элементов системы информационной безопасности корпоративной сети.
4) Разработать план развертывания системы обеспечения информационной безопасности корпоративной сети.

5) Разработать порядок настройки элементов системы информационной безопасности корпоративной сети.

5. 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. Основные понятия защиты информации и информационной безопасности.
2. Угрозы информационной безопасности.
3. Сетевой информационный обмен.
4. Угрозы сетевой безопасности.
5. Проблемы безопасности IP-сетей.
6. Угрозы и уязвимости проводных корпоративных сетей.
7. Угрозы и уязвимости беспроводных сетей.
8. Способы обеспечения информационной безопасности сетей.
9. Пути решения проблем защиты информации в сетях.
10. Структура политики безопасности организации
11. Базовая политика безопасности.
12. Специализированные политики безопасности.
13. Процедуры безопасности.
14. Роль стандартов информационной безопасности.
15. Международные стандарты информационной безопасности.
16. Стандарты ISO/IEC 17799:2002 (BS 7799:2000).
17. Германский стандарт BS1.
18. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий».
19. Стандарты для беспроводных сетей.
20. Стандарты информационной безопасности в Интернете.
21. Отечественные стандарты безопасности информационных технологий.
22. Симметричные криптосистемы шифрования.
23. Асимметричные криптосистемы шифрования.
24. Комбинированная криптосистема шифрования.
25. Электронная цифровая подпись и функция хэширования.
26. Основные процедуры цифровой подписи.
27. Функция хэширования.
28. Управление криптоключами.
29. Классификация криптографических алгоритмов.
30. Симметричные алгоритмы шифрования.
31. Основные понятия.
32. Блочные алгоритмы шифрования данных.
33. Асимметричные криптоалгоритмы.
34. Алгоритм шифрования RSA.
35. Алгоритмы цифровой подписи.
36. Аутентификация, авторизация и администрирование действий пользователей.
37. Методы аутентификации, использующие пароли и PIN-коды.
38. Аутентификация на основе многоразовых паролей.

39. Аутентификация на основе одноразовых паролей.
40. Аутентификация на основе PIN-кода.
41. Строгая аутентификация. Основные понятия.
42. Строгая аутентификация, основанная на симметричных алгоритмах.
43. Строгая аутентификация, основанная на асимметричных алгоритмах.
44. Биометрическая аутентификация пользователя.
45. Управление идентификацией и доступом.
46. Особенности управления доступом.
47. Функционирование системы управления доступом.
48. Организация защищенного удаленного доступа.
49. Протоколы аутентификации удаленных пользователей.
50. Централизованный контроль удаленного доступа.
51. Управление доступом по схеме однократного входа с авторизацией Single Sign-On (SSO).
52. Простая система однократного входа SSO.
53. SSO-продукты уровня предприятия.
54. Протокол Kerberos.
55. Инфраструктура управления открытыми ключами PKI.
56. Принципы функционирования PKI.
57. Логическая структура и компоненты PKI.
58. Концепция адаптивного управления безопасностью.
59. Технология анализа защищенности.
60. Средства анализа защищенности сетевых протоколов и сервисов.
61. Средства анализа защищенности ОС.
62. Технологии обнаружения атак.
63. Методы анализа сетевой информации.
64. Классификация систем обнаружения атак IDS.
65. Компоненты и архитектура IDS.
66. Компьютерные вирусы и проблемы антивирусной защиты.
67. Классификация компьютерных вирусов.
68. Жизненный цикл вирусов.
69. Основные каналы распространения вирусов и других вредоносных программ.
70. Антивирусные программы и комплексы.
71. Построение системы антивирусной защиты корпоративной сети.
72. Задачи управления системой сетевой безопасности.
73. Архитектура управления средствами сетевой безопасности.
74. Концепция глобального управления безопасностью.
75. Глобальная и локальная политики безопасности.
76. Функционирование системы управления средствами безопасности.
77. Аудит и мониторинг безопасности.