Оценочные материалы для промежуточной аттестации по дисциплине

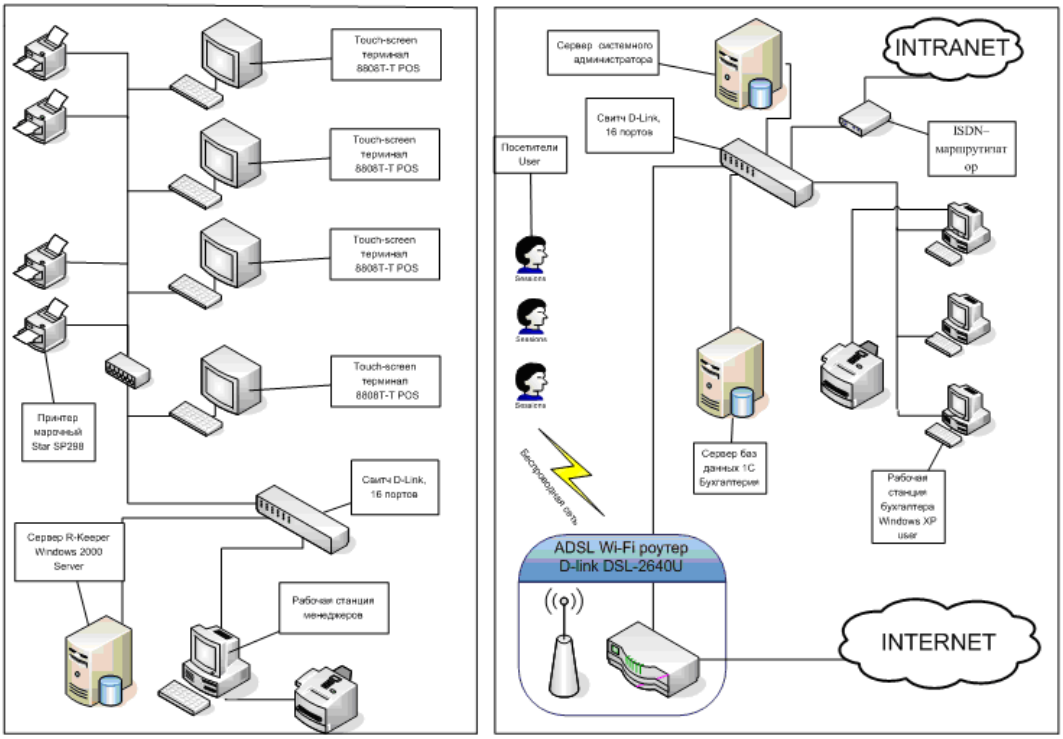
Безопасность сетевых технологий, 3 семестр

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. Сетевая безопасность. Основные понятия.
2. Типы и примеры атак.
3. Методы обеспечения информационной безопасности.
4. Межсетевые экраны и их особенности.
5. Использование межсетевых экранов. Фильтрующие маршрутизаторы.
6. Основные компоненты межсетевых экранов. Шлюзы сетевого и прикладного уровня.
7. Средства безопасности маршрутизаторов. NAT и Port Mapping (проброс портов). Демилитаризованная зона (DMZ-зона).
8. Виртуальные частные сети VPN. Понятие, особенности, настройка. Основные компоненты VPN-туннеля.
9. Виртуальные частные сети VPN. Понятие, особенности, настройка.
10. Виртуальные локальные сети VLAN. Понятие, особенности, настройка.
11. Защита на канальном уровне. Протоколы VPNсетей: PPTP, L2TP.
12. Безопасность информационных сервисов Интернет. Шифрование Интернет каналов. Защита на сетевом уровне: протокол IPSec.
13. Протокол SSL. Этапы установки SSL-соединения.
14. Протокол TLS. Этапы установки TLS-соединения.
15. Socks-прокси. Назначение и особенности.
16. Защита на прикладном уровне: протокол HTTPS.
17. Защита на прикладном уровне: протокол SSH.
18. Шифрование данных. Программное обеспечение для шифрования данных. Шифрование данных при хранении –файловая система EFS.
19. Использование протокола Radius. Методы аутентификации в компьютерной сети. Авторизация через Radius-сервер.
20. Применение технологии терминального доступа для организации защищенной компьютерной системы.
21. Аудит сетевой инфраструктуры. Общие сведения об аудите. Этапы аудита. Методики аудита. Технические средства аудита.
22. RAID-массивы и их виды.
23. Резервное копирование как способ защиты информации.
24. Политики безопасности. Локальная и групповая политики безопасности. Группы безопасностей инфокоммуникационных сетей. Типы групп безопасностей, их назначение. Встроенные группы безопасности.
25. Инструменты управления группами безопасности. Графические утилиты, утилиты командной строки. Права доступа в Windows и Linux.
26. Аутентификация в распределенных системах. Схема Kerberos. Применение схемы Kerberos.

27. Управление доступом к данным. Списки прав доступа к объектам операционной системы.
28. Групповые политики, функции и назначения. Объекты групповой политики. Назначение групповых политик для задач администрирования.
29. Создание и редактирование объектов групповой политики. Инструменты управления групповыми политиками.
30. Шаблоны безопасности. Примеры шаблонов. Инструменты управления политиками безопасности.
31. Контроллеры доменов, функции и назначение. Роли контроллеров. Репликация данных между контроллерами доменов. Протоколы репликации.
32. Утилиты командной строки для управления удаленным компьютером: просмотр информации об удаленной системе, запуск и остановка служб и приложений, остановка удаленной системы.
33. Объекты контроллеров домена. Инструменты управления объектами контроллеров домена.
34. Удаленное управление компьютером. Сервер терминалов. Сеансы пользователей. Управление многопользовательской средой. Инструменты управления.
35. Серверы БД. Системы управления базами данных. Административные задачи управления сервером БД.
36. Архитектура информационной безопасности сервера БД. Аутентификация в распределенной среде. Режимы аутентификации в SQL-сервере: проверка подлинности, проверка средствами SQL-сервера.
37. Информационная безопасность. Роли пользователей на уровне сервера БД. Назначение ролевой модели. Инструменты управления ролями пользователей.
38. Журналы транзакций БД. Инструменты создания, удаления и управления журналами транзакций. Операторы Transact-SQL
39. Резервное копирование и восстановление данных. Модели восстановления данных, их особенности. Стратегии резервного копирования и их связь с моделями восстановления.
40. Разграничение доступа к данным. Разрешения на уровне БД, таблиц, представлений, отдельных полей. Инструменты разграничения доступа к данным.
41. Веб-службы и веб-сервисы в Интернет. Основные протоколы прикладного уровня, используемые для передачи данных в Интернет. Клиент-серверные технологии. Провайдеры услуг Интернет. Информационная безопасность Веб-служб.
42. Веб-серверы. Основные понятия. Инструменты управления веб-службами. Командные скрипты управления веб-службами. Обеспечение информационной безопасности веб-серверов.
43. Сервисы FTP, функции и назначение. Создание и конфигурирование ftp-сервера. Инструменты управления, решение основных административных задач. Обеспечение информационной безопасности сервисов FTP.
44. Почтовые службы. Типы почтовых серверов. Настройка и обеспечение информационной безопасности SMTP-сервера.
45. Безопасность информационных систем. Политика информационной безопасности. Управление доступом к файловым ресурсам. Шифрование файловых ресурсов.

46. Цифровые сертификаты. Назначение, принцип работы, аутентификация. Назначение центра сертификации. Самоподписанные (самозаверенные) сертификаты.