Вопросы, выносимые на государственный экзамен

1. Угрозы ИБ. Основные понятия. Классификация угроз. Классификация источников угроз. Виды удалённых атак. Методы анализа уязвимости информационной системы.
2. Органы защиты государственной тайны. Организация режима защиты государственной тайны. Допуск предприятий, учреждений и организации к проведению работ, связанных с использованием сведений, составляющих государственную тайну. Основные положения допуска должностных лиц и граждан к государственной тайне: получение и прекращение допуска.
3. Поясните осуществление контроля и надзора за обеспечением защиты государственной тайны. Охарактеризуйте виды правовой ответственности за нарушения законодательства РФ «О государственной тайне». Перечислите и охарактеризуйте виды посягательств на государственную тайну
4. Охарактеризуйте положения ФЗ-152 «О персональных данных». Источники права. Основные термины. Документы, содержащие персональные данные. Регуляторы и их основные области деятельности в рамках исполнения ФЗ-152.. Ответственность за нарушение требований закона ФЗ-152.
5. Раскройте основные принципы и условия обработки персональных данных согласно ФЗ-152.
6. Институты правовой защиты конфиденциальной информации. Коммерческая тайна как объект права. Режим коммерческой тайны. Охрана конфиденциальности информации, составляющей коммерческую тайну. Ответственность за нарушение законодательства о коммерческой тайне.
7. Охарактеризуйте обеспечение информационной безопасности в организациях банковской ссистемы РФ ( СТО БР ИББС-1.0-2010).
8. Законодательство РФ по лицензированию и сертификации в области информационной безопасности. Дайте определение терминам «лицензия» и «лицензирование»
9. Поясните назначение сертификационно–испытательных центров и лабораторий. Поясните работу структуры сертификации средств защиты информации.
10. Основные нормативно-правовые акты в области лицензирования деятельности по технической защите конфиденциальной информации.
11. Раскройте суть термина «интеллектуальная собственность». Какие из существующих институтов права и какие субъекты интеллектуальной собственности занимаются регулированием вопросов интеллектуальной собственности?
12. Основные виды вредоносных программ. VirWare (классические вирусы и сетевые черви). TrojWare (троянские программы). Спам. Технологии рассылки спама. Технологии борьбы со спамом. Методы борьбы с вредоносными программами.
13. Условия существования вредоносных программ в конкретной ОС. Способы проникновения в вредоносных программ в ОС. Правила именования вредоносных программ. Способы защиты от вредоносных программ. Классификация вредоносных программ.
14. Назначение стандарта ГОСТ Р ИСО/МЭК 15408-2002. Основные определения, структура, применение.
15. Достоинства и недостатки симметричных и асимметричных методов шифрования
16. Эталонная модель взаимодействия открытых систем.
17. Структура АТМ-ячейки. Отличие заголовков АТМ для различных интерфейсов. Эталонная модель АТМ. Функции уровней и плоскостей эталонной модели АТМ.
18. Назначение стека протоколов PNNI.
19. Технологии беспроводного абонентского доступа (WLL). Область применения. Стандарты беспроводных телефонов.
20. Принципы помехоустойчивого кодирования. Циклические коды.
21. Принципы работы концентраторов,коммутаторов, маршрутизаторов. Опишите возможные сетевые атаки на коммутаторы (реализация и противодействие) - переполнение САМ-таблицы, VLAN-hopping, атака на STP, MAC-spoofing, атака на DHCP-сервер.
22. Суть технологии MPLS. Компоненты технология MPLS. Структура метки MPLS.
23. Локальные сети Ethernet - метод доступа к общей физической среде. Технологии FastEthernet, GigabitEthernet.
24. Особенности работы протокола BGP. Уязвимости протокола BGP и меры противодействия.
25. Адресация в сетях IP. Типы IP адресов. Классовая адресация. Бесклассовая адресация. Специальные IP-адреса. Частные IP-адреса.
26. Основные характеристики протокола IPv4. Структура заголовка протокола IPv4. Основные характеристики протокола ARP. Приведите заголовок протокола ARP.
27. Приведите основные характеристики протоколов ICMP и ARP, структуры заголовков.
28. Основные недостатки технологии IPv4, вследствие которых перешли к технологии IPv6. Структура заголовка IPv6.
29. Характеристики протокола TCP. Структура TCP пакета. Флаги TCP. Процесс установления соединения.
30. Особенности (уязвимости) функционирования протокола ТСР. Опишите возможные атаки и способы их предотвращения. Этапы реализации атаки К. Митника. Меры обеспечения безопасного функционирования протокола ТСР.
31. Характеристики протокола UDP. Заголовок протокола UDP. Основные характеристики и назначение протокола ICMP.
32. Приведите особенности (уязвимости) функционирования протоколов UDP, ICMP. Опишите возможные атаки. Меры обеспечения безопасного функционирования протоколов UDP, ICMP.
33. Технология SNMP. Основные характеристики протокола SNMP. Основные команды SNMP v.1, SNMP v.3, SNMP v.3.
34. Что понимают под виртуальными частными сетями (VPN). Каковы виды технической реализации VPN.
35. Назначение протокола IKE. Какие параметры SA определяются при работе IKE? Для чего необходимы криптоключи при функционировании VPN? Способы построения защищенного виртуального туннеля и этапы формирования.
36. Основные задачи протокола IPSec. Архитектура IPSec (опишите назначение каждого из компонентов, порядок их взаимодействия).
37. Базы данных и их функциональное назначение в структуре IPSec. Опишите этапы установления защищенного соединения при помощи IKE. Схемы реализации протокола IPSec.
38. Приведите порядок взаимодействия протоколов IPSec. Опишите назначение баз данных политик безопасности SPD и безопасных ассоциаций SAD, соединений Security Associations.
39. Опишите особенности реализации VPN сетевого уровня на примере протокола IPSec (основные задачи, компоненты).
40. Задача контроля и фильтрации межсетевого трафика. Определение межсетевого экрана. Структура межсетевого экрана.
41. Особенности протокола SSL. Опишите параметры безопасности, обеспечиваемые с помощью протокола SSL. Приведите схемы реализации протокола SSL. Этапы установления защищенного соединения при помощи SSL.
42. Модели безопасности: Дискреционная модель. Мандатная модель. Ролевая модель. Достоинства, недостатки.
43. Дайте краткую характеристику международного стандарта ISO/IEC 17799-2005. Характеристика разделов, назначение стандарта, достоинства и недостатки, его взаимосвязь с ISO/IEC 27001.
44. Управление рисками. Этапы управления рисками.Составляющие процесса управления.
45. Процедура «обработки риска» в СУИБ. Изобразите схему процесса обработки рисков ИБ.
46. Аудит информационной безопасности - цели, принципы, типы организации, требования к аудитору.
47. Приведите определения относящихся к процессу регистрации пользователей в информационной системе. Опишите компоненты аутентификации и их содержание. Поясните термин «Фактор аутентификации».
48. Дайте определения терминам - объект, субъект, монитор безопасности обращений. Математические модели используются для описания моделей доступа. Поясните основные свойства и элементы избирательного управления доступом. Достоинства и недостатки избирательного управления доступом.
49. Основные свойства и элементы полномочного управления доступом. Достоинства и недостатки полномочного управления доступом. Суть модели Белла-ЛаПадула.
50. Аутентификация пользователей информационных систем. Базовые понятия. Факторы аутентификации. Виды аутентификации. One-time password. Хэш-функция (практ. использование). Криптография с открытым ключом (практ. использование).
51. Методы идентификации и аутентификации в ОС. Механизм управления доступом в ОС.
52. Принцип парольной аутентификации. Стойкость парольной аутентификации? Процесс парольной аутентификации на основе хешированного пароля. Недостатки методов аутентификации с запоминаемым паролем и способы защиты.
53. Дайте определения биометрическим характеристикам. Какие коэффициенты показывают эффективность биометрических методов аутентификации? Приведите достоинства и недостатки биометрических методов аутентификации.
54. Поясните процесс аутентификации на основе ОТР-токенов. Поясните процесс аутентификации с помощью метода «запрос-ответ» при использовании ОТР-токенов. Недостатки методов аутентификации с помощью ОТР и способы защиты.
55. Парольная аутентификация. Достоинства и недостатки. Меры, позволяющие повысить надежность парольной аутентификации.
56. Охарактеризуйте виды правовой ответственности за нарушения законодательства РФ «О государственной тайне».
57. Ответственность за нарушение требований закона ФЗ-152.
58. Определения параметров ИБ согласно ГОСТ Р ИСО/МЭК 15408-2002
59. Методы защиты информации на канальном уровне модели взаимосвязи открытых систем
60. Методы защиты информации на сетевом уровне модели взаимосвязи открытых систем
61. Назначение мультиплексора, коммутатора, маршрутизатора, хоста, сервера, шлюза.
62. Общую классификация вредоносных программ. Типы вирусов и червей.
63. Основные способы обеспечения QoS в IP-сетях.
64. Виды услуг VPN и их схемы реализации.
65. Дайте определение термину безопасная ассоциация (security association), в чем состоит процедура установления SA.