Экзаменационные вопросы по предмету
Методы и средства защиты компьютерной информации

1. Защита информации. Основные понятия. Угрозы и меры защиты. Виды атак. Лица, атакующие компьютеры и сети.
2. Локальные атаки. Методы защиты. Устройства идентификации пользователя на основе физических носителей.
3. Локальные атаки. Методы защиты. Устройства идентификации пользователя на основе физических параметров.
4. Сетевые атаки. Атаки на Web-браузеры и сайты. Методы защиты.
5. Сетевые атаки. Атаки на электронную почту. Методы защиты.
6. Сетевые атаки. Атаки на сервис обмена мгновенными сообщениями. Методы защиты.
7. Сетевые атаки. Перехват данных. Снифинг. Включение в разрыв сети. Методы защиты.
8. Сетевые атаки. Перехват данных. Ложные запросы. Перехват TCP-соединения. Методы защиты.
9. Сетевые атаки. Перехват данных в радиосетях. Современные технологии защиты.
10. Сетевые атаки. Атаки на отказ в обслуживании. Цели и основные методы атак. Атака насыщением полосы пропускания. Методы защиты.
11. Сетевые атаки. Атаки на отказ в обслуживании. Цели и основные методы атак. Атака на истощение ресурсов. Методы защиты.
12. Сетевые атаки. Атаки на отказ в обслуживании. Цели и основные методы атак. Атака некорректными сетевыми пакетами. Методы защиты.
13. Сетевые атаки. Атаки на отказ в обслуживании. Цели и основные методы атак. Атаки фальсифицированными сетевыми пакетами. Методы защиты.
14. Социальная инженерия. Сферы применения. Примеры методов атак. Рекомендации по защите.
15. Стеганография. Классические и компьютерные методы стеганографии. Область применения.
16. Криптография. Основные термины и определения. Задачи криптографии.
17. Шифрование данных. Основные термины и определения. Классификация алгоритмов шифрования.
18. Поточные шифры простой замены. Классификация. Примеры. Методы криптоанализа.
19. Блочные шифры простой замены. Методы криптоанализа блочных шифров простой замены. Шифры Плейфера и Хилла.
20. Блочные шифры простой замены. Методы криптоанализа блочных шифров простой замены. Американские стандарты шифрования DES, AES и российский ГОСТ-28147-89, алгоритм IDEA.
21. Шифры гаммирования. Шифр Виженера. Одноразовые блокноты. Методы криптоанализа.

22. Шифры перестановки. Примеры. Методы криптоанализа.

23. Асимметричные системы шифрования. Основной принцип работы. Система шифрования RSA. Методы криптоанализа и защиты.

24. Обеспечение целостности. Код аутентификации сообщения. Требования и средства реализации.

25. Ключевые хэш-функции. Основные требования и примеры построения. Атаки на хеш-функции.

26. Бесключевые хэш-функции. Основные требования и примеры построения. Атаки на хэш-функции. Хэш-функция MD5.

27. Бесключевые хэш-функции. Основные требования и примеры построения. Атаки на хэш-функции. Хэш-функция SHA-1.

28. Обеспечение аутентификации. Протоколы идентификации. Классификация протоколов. Основные виды атак на протоколы идентификации и методы защиты.

29. Парольная идентификация. Методы атак и защиты.

30. Идентификация «запрос-ответ». Методы атак и защиты.

31. Обеспечение неоспоримости. Цифровая подпись. Задачи и алгоритмы реализации. Вычисление цифровой подписи на основе специальных алгоритмов. Цифровая подпись Фиата — Шамира.

32. Обеспечение неоспоримости. Цифровая подпись. Задачи и алгоритмы реализации. Вычисление цифровой подписи на основе специальных алгоритмов. Цифровая подпись ГОСТ Р 34.10-2001 (на основе эллиптических кривых).

33. Симметричные и асимметричные алгоритмы вычисления цифровой подписи. Схемы цифровой подписи с восстановлением и дополнением.

34. Информационная безопасность. Определение и основные задачи. Политика информационной безопасности. Составные элементы политики информационной безопасности.

35. Информационная безопасность. Механизмы и инструменты информационной безопасности.

36. Информационная безопасность. Основные направления. Служба информационной безопасности. Критерии необходимости создания службы.

37. Методы контроля физического доступа. Классификация, основные механизмы и задачи. Живучесть системы безопасности.

38. Протоколы сетевой безопасности. Задачи. Протоколы PPP и PAP.

39. Протоколы сетевой безопасности. Задачи. Протоколы SHTTP, SSL.

40. Протоколы сетевой безопасности. Задачи. Протоколы S/Key, Kerberos.

41. Автоматизированные средства безопасности. Антивирусы. Межсетевые экраны.

42. Автоматизированные средства безопасности. Технологии VPN и VLAN.

43. Автоматизированные средства безопасности. Сканеры уязвимостей. Системы обнаружения атак. Классификация систем обнаружения атак.

44. Автоматизированные средства безопасности. Системы Honey-Pot и Honey-Net. Область применения и задачи. Принцип построения и функционирования.

Экзаменационные задачи по предмету

Методы и средства защиты компьютерной информации

1. Расшифровать сообщение, зашифрованное аффинным шифром, если известно, что буква «X1» шифротектса, соответствует букве «Y1» открытого текста, а буква «X2» шифротектса, соответствует букве «Y2» открытого текста,.
2. Расшифровать сообщение, зашифрованное алгоритмом Плейфера.
3. Расшифровать сообщение, зашифрованное алгоритмом Хилла.
4. Расшифровать сообщение, зашифрованное алгоритмом RSA.
5. Расшифровать сообщение, зашифрованное шифром вертикальной перестановки.