Перечень вопросов для подготовки к экзамену
по дисциплине «Защита компьютерной информации»

1. Дайте основные понятия и определения информационной безопасности.
2. Какие основные угрозы безопасности компьютерных систем вы знаете? Приведите механизмы защиты компьютерных систем.
3. Что такое криптография? Перечислите принципы криптографической защиты информации
4. Дайте понятие классические симметричные криптосистемы.
5. Опишите историю развития криптографии.
6. Опишите шифрование с использованием метода шифрующих таблиц. Приведите примеры.
7. Опишите шифрование с использованием метода магического квадрата. Приведите примеры.
8. Опишите шифрование с использованием систем Цезаря. Приведите примеры.
9. Опишите шифрование с использованием системы Трисемуса. Приведите примеры.
10. Опишите шифрование с использованием шифра «двойной квадрат» Уитстона. Приведите примеры.
11. Опишите шифрование с использованием шифра Бофора. Приведите примеры
12. Опишите шифрование с использованием системы Вижинера. Приведите примеры.
13. Какие современные симметричные криптосистемы вы знаете. Опишите американский стандарт шифрования DES.
14. Какие современные симметричные криптосистемы вы знаете. Опишите блочные и поточные шифры.
15. Дайте понятие асимметричной криптосистемы.
16. Опишите криптосистему RSA
17. Опишите схему шифрования Полига-Хеллмана
18. Опишите схему шифрования Эль-Гамаля
19. Опишите термины и обозначения схемы шифрования ГОСТ 28147-89
20. Опишите логику построения шифра и структура ключевой информации ГОСТа 28147-89
21. Опишите базовые циклы криптографических преобразований в системе шифрования ГОСТ 28147-89
22. Дайте основные понятия и концепции идентификации и аутентификации пользователей
23. Какие способы взаимной проверки подлинности пользователей вы знаете?
24. Дайте краткое описание протоколов идентификации с нулевой передачей данных
25. Дайте Понятие ЭЦП. Что такое однонаправленные хэш-функции?
26. Опишите реализация элементов ЭЦП RSA
27. Опишите реализация элементов ЭЦП EGSA
28. Опишите реализация элементов ЭЦП DSA
29. Опишите реализация элементов ЭЦП RSA
30. Опишите термины и обозначения схемы шифрования ГОСТ Р 34.10-94
31. Опишите логику построения шифра и структура ключевой информации ГОСТа Р 34.10-94
32. Опишите подходы к организации разграничения доступа к информации в компьютерных системах.
33. Какие современные системы защиты ПЭВМ от несанкционированного доступа к информации вы знаете?
34. Опишите шифрование данных с использованием программного средства PGP
35. Приведите примеры ПО для шифрования/дешифрования отдельных файлов, отдельных дисков и всего винчестера
36. Опишите создание виртуальных зашифрованных дисков (программное средство TrueCrypt)
37. Опишите, как можно организовать срытие данных на винчестере.
38. Опишите концепцию адаптивного управления безопасностью.
39. Опишите технологию анализа защищенности
40. Опишите технологию обнаружения атак
41. Опишите угрозы безопасности ОС. Раскройте понятие «Архитектура подсистемы защищенной ОС»
42. Опишите методы и средства защиты от удаленных атак через сеть Internet.
43. Раскройте особенности функционирования межсетевых экранов
44. Какие способы защита информации в электронных платежных системах вы знаете?
45. Какие способы защита информации в программном обеспечении государственных органов и организаций Республики Беларусь вы знаете?
46. Какие встроенные функции защиты предлагает Microsoft Office.
47. Какие методы симметричного шифрования Вы знаете?
48. В чем достоинства и недостатки алгоритма RSA?

49. Дайте понятие компьютерная стеганография? Опишите основные особенности реализации компьютерной стенографии?
50. Дайте определение понятию шифрование «на лету»?
51. Опишите обеспечение безопасности систем POS.
52. Опишите обеспечение безопасности банкоматов и интернет банкинга.
53. Опишите универсальную платежную систему UEPS.
54. Дайте понятие аппаратно-программные средства защиты информации
55. Опишите современные приложения криптографии.
56. Опишите классификация методов криптографического закрытия.