Вопросы к Гос. экзамену с исправлениями (2018)

1. Акустические каналы утечки информации. Способы и средства защиты речевой информации от утечки.
2. Аттестация объектов информатизации (ОИ) по требованиям безопасности информации: организационная структура системы аттестации ОИ, функции участников.
3. Безопасность виртуальной вычислительной среды.
4. Безопасность облачных вычислений.
5. Блочный шифр «Кузнечик» ГОСТ Р 34.12-2015.
6. Блочный шифр «Магма» ГОСТ Р 34.12-2015.
7. Государственные информационные системы. Требования безопасности и меры защиты.
8. Задачи, решаемые VPN. Туннелирование в VPN. Защита данных на канальном, сетевом и транспортном уровне.
9. Источники угроз безопасности информации. Внешние и внутренние угрозы. Способы реализации угроз безопасности информации на объектах информатизации.
10. Каналы силового деструктивного воздействия на информацию. Средства защиты.
11. Классификация технической разведки по физической природе носителя. Способы и средства добывания информации техническими средствами.
12. Классификация угроз безопасности информации. Построение и документальное оформление комплексной модели угроз безопасности информации на предприятии.
13. Классы защищенности автоматизированных систем от несанкционированного доступа.
14. Компьютерные вирусы как особый класс разрушающих программных средств: классификация, методы внедрения.
15. Криптографическая система. Алгебраическая и вероятностная модель шифра. Классификация криптосистем.
16. Криптографические хэш-функции. Хэш-функция ГОСТ Р 34.11-2012.
17. Криптографический алгоритм AES.
18. Криптосистемы с открытым ключом. Криптографический алгоритм RSA.
19. Материально-вещественные каналы утечки информации. Способы предотвращения утечки информации.
20. Методы и средства обеспечения защиты информации от несанкционированного доступа.
21. Модель измерений информационной безопасности ISO/IEC 27004
22. Модель нарушителя. Уровни и категории нарушителя.
23. Общая характеристика уязвимостей информационной системы.
24. Общие подходы к оценке рисков информационной безопасности: определение риска, стратегии анализа риска, определение величины (уровня) риска, определение приемлемости риска.
25. Обязанности администратора по обеспечению безопасности информации.
26. Оптические каналы утечки информации. Способы и средства противодействия наблюдению в оптическом диапазоне.
27. Организация пропускного режима: цели и задачи пропускного режима, основные элементы системы организации пропускного режима.
28. Основные нормативные правовые акты РФ в области защиты информации, их назначение, краткое содержание.

29. Основные организационно-распорядительные документы по защите информации в организации, их назначение, краткое содержание.
30. Основные организационные мероприятия по защите информации.
31. Основные принципы криптографии на эллиптических кривых. Система электронной подписи ГОСТ Р 34.10-2012.
32. Основные технические мероприятия по защите информации.
33. Оценка информационной безопасности компании: этапы проведения и роли в процессе оценки.
34. Побочные электромагнитные излучения и наводки (ПЭМИН). Защита информации от утечки по каналам ПЭМИН.
35. Политика и система обеспечения информационной безопасности РФ, функции государственных регулирующих органов в сфере обеспечения ИБ РФ.
36. Политика информационной безопасности организации: принципы разработки, иерархическая структура документов, основное содержание.
37. Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак.
38. Порядок создания, аттестации и эксплуатации защищаемых (выделенных) помещений, рекомендации по размещению.
39. Построение и принципы работы типовых антивирусных средств.
40. Построение системы менеджмента информационной безопасности на основе ISO/IEC 27001-2006: основные этапы цикла управления, определение области действия (границ), сертификация соответствия.
41. Правовой режим коммерческой тайны, требования основных нормативных правовых актов РФ о коммерческой тайне.
42. Правовые основы электронного документооборота. Федеральный закон «Об электронной подписи».
43. Радиоэлектронные каналы утечки информации. Способы и средства противодействия радиоэлектронному и акусто-радиоэлектронному наблюдению.
44. Реализация управления доступом средствами операционной системы. Защита информации в операционных системах Windows.
45. Реализация управления доступом средствами операционной системы. Защита информации в операционных системах семейства UNIX.
46. Режимы работы блочных шифров ГОСТ Р 34.13-2015.
47. Симметричные композиционные шифры: принципы синтеза и основные схемы.
48. Система лицензирования деятельности в области защиты информации. Цели и задачи лицензирования.
49. Системы обнаружения вторжений (СОВ). Классификация, стандартизация, типовая архитектура СОВ.
50. Системы электронной подписи. Детерминированные и рандомизированные цифровые подписи.
51. Создание автоматизированных систем (АС) в защищённом исполнении. Цель и основные этапы создания.
52. Состав государственной системы защиты информации от инженерно-технической разведки и от утечки информации по техническим каналам, функции и задачи.
53. Способы защиты программного обеспечения от копирования.
54. Принципы инженерно-технической защиты информации.
55. Способы и средства обеспечения целостности информации.

56. Способы и средства предотвращения утечки информации при использовании нарушителем закладных устройств.
57. Способы идентификации и аутентификации субъектов компьютерных систем.
58. Средства поиска и удаления остаточной информации на магнитных носителях информации.
59. Стандарты управления информационной безопасностью. Структура и состав серии стандартов ISO/IEC 27000, особенности применения в РФ.
60. Стратегии и средства межсетевого экранирования. Требования руководящих документов ФСТЭК России к межсетевым экранам.
61. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники.
62. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Сигнатурный анализ и обнаружение аномалий
63. Виды оценки информационной безопасности компании. Аудит информационной безопасности организации.
64. Требования нормативных правовых актов РФ о государственной тайне: организация допуска к сведениям, составляющим государственную тайну.
65. Требования нормативных правовых актов РФ о государственной тайне: принципы и порядок отнесения сведений к государственной тайне, степени и грифы секретности.
66. Требования основных нормативных правовых актов РФ в области обеспечения безопасности персональных данных.
67. Управление рисками информационной безопасности на основе ISO/IEC 27005: итерационная процедура управления рисками, этапы оценки рисков.
68. Управление рисками информационной безопасности на основе ISO/IEC 27005: обработка риска, понятие остаточного риска, критерии принятия риска.
69. Федеральный закон «Об информации, информационных технологиях и защите информации». Правовые основы ограничения доступа к информации.
70. Формальные модели разграничения доступа. Дискреционные модели. Мандатные модели.
71. Цели и задачи аудита безопасности компьютерных систем. Этапы и методы проведения, нормативно-правовые и организационные основы проведения аудита безопасности.
72. Цели и классификация атак на алгоритмы шифрования, основные методы криптоанализа симметричных блочных шифров.
73. Цели, задачи, принципы построения и составные части комплексной системы защиты информации на предприятии.
74. Состав и характеристика единовременных затрат на обеспечение мероприятий по защите информации.
75. Состав и характеристика эксплуатационных затрат на обеспечение мероприятий по защите информации.