

**ВОПРОСЫ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ
ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ
ДЛЯ ПОСТУПАЮЩИХ В БЕЛГОРОДСКИЙ УНИВЕРСИТЕТ
КООПЕРАЦИИ, ЭКОНОМИКИ И ПРАВА
ПО ПРОГРАММЕ ПОДГОТОВКИ
НАУЧНО-ПЕДАГОГИЧЕСКИХ КАДРОВ В АСПИРАНТУРЕ
ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ
10.06.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) «МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ
ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

1. Что понимается под термином «информационная безопасность»?
2. Какие имеются основные направления в плане информационной безопасности?
3. Каковы основные функции ФСТЭК России?
4. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации.
5. Каковы функции информационно-телекоммуникационной системы специального назначения (ИТКС) и из каких основных комплексов она состоит?
6. Какие основные мероприятия проведены в государственных структурах, направленные на обеспечение информационной безопасности их функционирования?
7. Какова роль и основные функции государственных организаций и учреждений, научно-исследовательских организаций и учебных заведений в области обеспечения информационной безопасности страны.
8. Что понимается под термином «политика безопасности»?
9. Каковы основные функции мониторинга системы защиты, и какими средствами он реализуется?
10. Какие противоречивые задачи решаются при создании автоматизированной системы обработки данных?
11. Каковы наиболее распространенные политики безопасности и какими существенными признаками они отличаются друг от друга?
12. Как производится управление информационными потоками?
13. Объясните сущность концепции иерархической декомпозиции системы и особенности ее применения.
14. Каковы механизмы защиты, входящие в состав достоверной вычислительной базы и их свойства?
15. Каковы основные функции, выполняемые ядром безопасности совместно с другими службами операционной системы?
16. Перечислите основные принципы реализации политики безопасности.
17. Что такое внутренняя и внешняя безопасность АСОД?
18. Каковы причины случайного воздействия на АСОД? Перечислите и

объясните сущности угроз безопасности АСОД?

19. Что такое информационная интегральная безопасность АСОД?
20. Что такое стратегия защиты и в чем состоит суть анализа риска?
21. Каковы угрозы системе передачи данных?
22. Что подразумевается под оценкой безопасности системы?
23. Укажите основные нормативные документы ФСТЭК России, используемые при классификации средств защиты информации?
24. Укажите основные нормативные документы ФСТЭК России, используемые для защиты персональных данных?
25. Укажите основные нормативные документы ФСТЭК России, используемые для защиты государственных информационных систем?
26. Охарактеризуйте дискреционную модель разграничения доступа субъектов и процессов к данным?
27. Охарактеризуйте мандатную модель разграничения доступа субъектов и процессов к данным?
28. Охарактеризуйте классы защищенности автоматизированных систем от НСД к информации?
29. Состав и функции сотрудников административной группы управления защитой.
30. Объясните сущность жизненного цикла информации.
31. Информация как объект права собственности.
32. Каковы методы защиты информации от преднамеренного доступа при использовании простых средств хранения и обработки информации?
33. Что значит разграничение и контроль доступа к информации?
34. Охарактеризуйте термин «авторизация». Опишите наиболее распространенные способы авторизации пользователей в информационных системах. Каковы их особенности?
35. Как реализуются наиболее распространенные методы преодоления подсистемы авторизации?
36. Объясните суть комплексного подхода к организации систем защиты данных с применением только программных средств.
37. Какие защитные меры применяются при защите информации от побочного электромагнитного излучения и наводок?
38. Какие методы функционального контроля вычислительных систем Вы знаете?
39. Каковы методы защиты информации от преднамеренного доступа при использовании простых средств хранения и обработки информации?
40. Из чего состоит комплекс средств автоматизации и как организуется его обслуживание?
41. Каковы современные основные методы защиты информации в вычислительных системах?
42. Объясните суть комплексного подхода к организации систем защиты данных с применением только программных средств.
43. Какие защитные меры применяются при защите информации от

побочного электромагнитного излучения и наводок?

44. Какие методы функционального контроля вычислительных систем Вы знаете?

45. Каковы основные задачи криптографии в настоящее время?

46. Определите понятие «криптографический алгоритм».

47. Что собой представляет криптосистема?

48. Какие основные типы криптосистем знаете?

49. Дайте общее определение электронной цифровой подписи.

50. Объясните суть преобразований - перестановка и замена.

51. Что собой представляет симметричная криптографическая система?

52. Что собой представляет блочная симметричная криптографическая система?

53. Объясните, что такое композиционный блочный шифр и итерационный блочный шифр.

54. Отечественный алгоритм криптографического преобразования данных (ГОСТ 28147-90) и его отличительные особенности.

55. Какие режимы имеет отечественный алгоритм криптографического преобразования данных (ГОСТ 28147-90)?

56. Что подразумевается под понятием «вычислительная сложность алгоритма»?

57. Чем характеризуются односторонние функции с секретом?

58. Чем отличается криптографическая система с открытым ключом

59. Каков алгоритм криптографического преобразования с открытым ключом RSA, и каковы его характеристики?

60. На чем основывается проверка подписи, сформированной по схеме Эль Гамала?

61. Что такое хэш-функция? Чем отличаются хэш-функции с ключом и без ключа?

62. Какие основные отличительные особенности исторических этапов создания механизмов защиты информации, а также разработки средств, способов и методов защиты, применяемых в системах защиты?

63. Концепции защиты информации.

64. Какова концептуальная основа построения защиты информации вычислительных системах?

65. Вычислительная система как объект защиты.

66. Каковы потенциальные угрозы в вычислительной системе?

67. Каковы концептуальные основы построения системы защиты в вычислительной системе?

68. Охарактеризуйте возможные каналы несанкционированного доступа в вычислительной системе.

69. Общий алгоритм проектирования и разработки системы защиты информации в ВС.

70. Каковы основные мероприятия по предупреждению и контролю НСД в ВС?

71. Каковы концептуальные основы проектирования защиты информации от НСД в вычислительной сети и АСУ?
72. Каковы основные требования в области защиты информации в вычислительных сетях?
73. Укажите состав средств и структуру системы защиты информации от НСД в комплексах средств автоматизации.
74. Каковы основные характеристики потенциального нарушителя?
75. Из чего состоит модель элементарного нарушителя и как определяется прочность преграды (по вариантам)?
76. Как определяется прочность защиты при наличии у преграды нескольких обходных путей?
77. Как функционирует автоматизированная преграда (объясните поврежденной диаграмме контроля НСД)?
78. Как определяется прочность преграды при использовании организационных мер защиты?
79. Каким образом определяется прочность преграды защиты при учете отказа системы?
80. Как определяется суммарная прочность дублированных преград в многозвенной защите?
81. Что представляет собой эталонная модель взаимодействия открытых систем?
82. Укажите основные принципы построения системы защиты информации в сетях.
83. ЛВС как объект защиты информации.
84. Какие средства управления защитой информации ЛВС Вы знаете?
85. Что знаете об антивирусных средствах?
86. Укажите основные сервисные службы защиты информации, рекомендованные OSI.
87. Что Вы знаете об архитектуре клиент-сервер и о ее безопасности?
88. Какие функции выполняются межсетевыми экранами?
89. Какие имеются разновидности межсетевых экранов?
90. Чем отличаются прокси-серверы?
91. Какие имеются основные программные средства, обеспечивающие безопасность в сетях?
92. Какие задачи решает организационная защита информации?