Вариант 2

1. По какой причине удостоверяющий центр отзывает сертификат?
   1) Если открытый ключ пользователя скомпрометирован
   2) Если пользователь переходит на использование модели PEM, которая использует сеть доверия
   3) Если закрытый ключ пользователя скомпрометирован
   4) Если пользователь переходит работать в другой офис

2. Метод шифрования, в котором коды символов открытого текст складываются с элементами случайной или псевдослучайной последовательности называется
   1) Перестановкой
   2) Подстановкой
   3) Заменой
   4) Гаммированием

3. Какая криптосистема применяется для открытого распределения ключей симметричного шифрования?
   1) RSA
   2) EG
   3) DH
   4) DSA

4. Что из перечисленного ниже лучше всего описывает удостоверяющий центр?
   1) Организация, которая выпускает закрытые ключи и соответствующие алгоритмы
   2) Организация, которая проверяет процессы шифрования
   3) Организация, которая проверяет ключи шифрования
   4) Организация, которая выпускает сертификаты открытых ключей

5. Функции, для которых легко найти функцию прямого отображения и вычислительно сложно найти обратное называется:
   1) Линейные функции
   2) Нелинейные функции
   3) Односторонние функции
   4) Обратные функции

6. Установление санкционированным получателем (приемником), того факта, что полученное сообщение послано санкционированным отправителем (передатчиком) называется:

1) Идентификацией
2) Аутентификацией
3) Авторизацией
4) Контролем

7. Как проверить, что самоподписанный сертификат был модифицирован?

1) Запросить удостоверяющий центр, выдавший сертификат
2) Проверить цифровую подпись сертификата с помощью открытого ключа из этого сертификата
3) Внедрить открытый ключ в сертификат, вычислить хэш-значение от результата, сравнить полученное хэш значение с цифровой подписью
4) Все перечисленные способы пригодны

8. В чем преимущество RSA над DSA?

1) Он может обеспечить функциональность цифровой подписи и шифрования
2) Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
3) Это блочный симметричный шифр и он лучше поточного
4) Он использует одноразовые шифровальные блокноты

9. Системы, где с помощью открытого ключа шифрую ключ симметричного криптоалгоритма, а само сообщение шифруют с помощью этого секретного ключа, называют:

1) Ассиметричные криптосистемы
2) Системы цифровой подписи
3) Гибридные криптосистемы
4) Симметричные криптосистемы

10. Какой из перечисленных ниже алгоритмов основан на сложности задачи дискретного логарифмирования?

1) MD5
2) DH
3) AES
4) RSA

11. Чему равна разрядность ключа алгоритма Магма? (Неточный вопрос)
    1) 58 бит
    2) 64 бит
    3) 128 бит
    4) 256 бит

12. Что используется для создания цифровой подписи?
    1) Закрытый ключ получателя
    2) Открытый ключ отправителя
    3) Закрытый ключ отправителя
    4) Открытый ключ получателя

13. Какова эффективная длина ключа 3DES в схеме EDE2?
    1) 56 бит
    2) 112 бит
    3) 128 бит
    4) 256 бит

14. При использовании классических криптографических алгоритмов ключ шифрования и ключ расшифрования совпадают и такие криптосистемы называются:
    1) Простыми криптосистемами
    2) Гибридными криптосистемами
    3) Ассиметричными криптосистемами
    4) Симметричными криптосистемами

15. Что необходимо иметь получателю для проверки электронной подписи на документе отправителя?
    1) Сертификат открытого ключа отправителя
    2) Сертификат открытого ключа получателя
    3) Собственный закрытый ключ
    4) Закрытый ключ отправителя

16. Какой из перечисленных ниже алгоритмов основан на сложности разложения больших чисел на два исходных простых сомножителя?

1) ECC
2) RSA
3) DES
4) DH

17. Чему равна допустимая разрядность ключа алгоритма шифрования Кузнечик (ГОСТ 34.12-15)?

1) 128 бит
2) 256 бит
3) 512 бит
4) Все варианты

18. Какой из перечисленных ниже алгоритмов использует симметричный ключ и алгоритм хэширования?

1) HMAC
2) 3DES
3) DSA
4) RSA

19. Какой ключ используется для зашифрования информации в ассиметричной криптосистеме?

1) Закрытый ключ получателя
2) Закрытый ключ отправителя
3) Открытый ключ получателя
4) Открытый ключ отправителя

20. Для чего используется протокол «Цербер» (Kerberus)?

1) Для несимметричной аутентификации
2) Для симметричной аутентификации
3) Для создания цифровой подписи
4) Для шифрования

21. Какова цель атаки «предсказания дополнения» на блочный симметричный шифр?

1) Подбор симметричного ключа
2) Расшифровка блоков сообщения
3) Определение длины и значения дополнения
4) Иной вариант

22. Совокупность действий, выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата называется:

1) Алгоритмом
2) Шифрованием
3) Расшированием
4) Протоколом

23. Какова цель атаки на гибридную криптосистему?

1) Подбор симметричного ключа
2) Подбор закрытого ключа отправителя
3) Подбор закрытого ключа получателя
4) Расшифровка сообщения

24. Что из перечисленного ниже лучше всего описывает цифровую подпись?

1) Это метод переноса собственноручной подписи на электронный документ
2) Это метод шифрования конфиденциальной информации
3) Это метод, обеспечивающий электронную подпись и шифрование
4) Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения

25. Какой атаке подвержены классические ассиметричные криптосистемы?

1) Атака посредника
2) Атака «встреча по середине»
3) Атака предсказания дополнения
4) Атака «грубой силы»

ChatGPT-4o
True

ВОЗМОЖНЫ ПОВТОРЕНИЯ ВОПРОСОВ – при повторении вопроса с банком который ниже, ответ выделяется ярко-зеленым.

ДА ЦВЕТА ПЛОХО РАЗЛЕЧИМЫ – но для тех, кто не составлял этот документ, цвета не должны иметь значения; если покрашено – значит правильно.

В банке вопросов ниже логотипа, представлен ТОЛЬКО ПРАВИЛЬНЫЙ ОТВЕТ.

0361

HOLD ON

1. Что является целью криптоанализа?
   Определение стойкости алгоритма

2. Частота применения брутфорс-атак возросла, поскольку:
   Мощность и скорость работы процессоров возросла

3. Что из перечисленного ниже не является свойством или характеристикой односторонней функции хэширования?
   Она преобразует сообщение фиксированной длины в значение переменной длины

4. Что может указывать на изменение сообщения?
   Изменился дайджест сообщения

5. Какой из перечисленных ниже алгоритмов является алгоритмом американского правительства, предназначенным для создания безопасных дайджестов сообщений?
   Secure Hash Algorithm

6. Что из перечисленного ниже лучше всего описывает отличия между HMAC и CBC-MAC?
   HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC

7. Многие страны ограничивают использование и экспорт криптографических систем. Зачем они это делают?
   Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования

8. Какова эффективная длина ключа в DES?
   56

9. Как расшифровывается аббревиатура DEA?
   Data Encryption Algorithm

10. Кто участвовал в разработке первого алгоритма с открытыми ключами?
    Мартин Хеллман

11. Какой процесс обычно выполняется после создания сеансового ключа DES?
    Обмен ключом

12. Сколько циклов перестановки и замещения выполняет DES?

16

13. Что из перечисленного ниже является правильным утверждением в отношении шифрования данных, выполняемого с целью их защиты?

Оно требует внимательного отношения к процессу управления ключами

14. Как называется ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст

Кластеризация ключей

15. Что из перечисленного ниже является определением фактора трудозатрат для алгоритма?

Время, которое займет взлом шифрования

16. Что является основной целью использования одностороннего хэширования пароля пользователя?

Это предотвращает ознакомление кого-либо с открытым текстом пароля

17. Что из перечисленного ниже описывает разницу между алгоритмами DES и RSA?

DES — это симметричный алгоритм, а RSA - асимметричный

18. Генерация ключей, для которой используются случайные значения, называется Функцией генерации ключей (KDF). Какие значения обычно не используются при этом в процессе генерации ключей?

Асимметричные значения

19. Функция называется односторонней функцией с секретом, если

Существует эффективный алгоритм вычисления значения функции для любого аргумента, а также существует эффективный алгоритм обращения функции, но только при знании некоторой дополнительной информации

20. Алгоритм безопасного хэширования (SHA) создает хэш-значение длиной

160 бит

21. Какая схема электронной цифровой подписи уязвима к мультипликативной атаке?

RSA

22. Пусть M - блок открытого текста, C - соответствующая ему криптограмма, e - открытый ключ алгоритма RSA, d - секретный ключ, N - модуль, тогда уравнение шифрования RSA есть:

$C=M^e \pmod N$

23. В качестве хэш-функции в стандарте цифровой подписи DSS (Digital Signature Standard) используется
SHA

24. Алгоритм хэширования ГОСТ Р 34.11-94 создает хеш-значение длиной
256 бит

25. Какая схема электронной цифровой подписи построена на сложности решения задачи дискретного логарифмирования на эллиптической кривой?
ГОСТ Р 34.10-2001

26. Аффинный шифр Цезаря является
Шифром простой замены

27. Режим применения блочного шифра, при котором любой входной поток преобразуется к значению фиксированной длины, являющемуся криптографической контрольной суммой
Выработки имитовставки

28. С помощью только электронной цифровой подписи невозможно обеспечить
Конфиденциальность

29. Опосредованной угрозой информационной
Угроза раскрытия параметров системы

30. Шифром, имеющим архитектуру «квадрат», является
Rijndael

31. Попытка получения злоумышленником информации, для просмотра которой у него нет разрешения называется
Атакой доступа

32. Последовательность, вырабатываемая криптографическим генератором псевдослучайных последовательностей, должна быть (укажите наиболее полный ответ)
Похожей на случайную (удовлетворять всем статистическим тестам на случайность), непредсказуемой

33. Гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано:

Надежность

34. Режим гаммирования ГОСТ 28147-89 соответствует
OFB

35. Наиболее эффективной является
Криптоаналитическая атака с адаптивным выбором открытого текста

36. Режим применения блочного шифра, при котором шифрование текущего блока зависит только от самого блока и искажение одного бита при передаче портит весь текущий блок:
ECB

37. Совокупность методов преобразования данных, направленная на то, чтобы сделать эти данные бесполезными для злоумышленника называется
Криптографией

38. Фактическая длина ключа шифрования алгоритма DES составляет
56 бит

39. Гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения постоянно выполняются:
Контроль доступа

40. Шифр скитала является
Шифром перестановки

41. Режим применения блочного шифра, при котором шифрование текущего блока зависит только от его расположения, искажение одного бита при передаче портит весь только один соответствующий бит:
OFB

42. Все возможные воздействия на автоматизированную систему обработки информации, которые прямо или косвенно могут нанести ущерб ее безопасности называются:
Угрозами информационной безопасности

43. Для реализации электронной цифровой подписи применяются
Криптосистемы с открытым ключом

44. Гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает:

Контроль аутентификации

45. Режим применения блочного шифра, при котором шифрование текущего блока зависит от текущего и всех предыдущих блоков, причем дополнение некратного последнего блока не нужно:
CFB

46. Известно, что полином x5+x2+1 является примитивным. Укажите период регистра сдвига с линейной обратной связью, у которого отводная последовательность соответствует данному полиному.
31~

47. Основной цикл шифрования/расшифрования алгоритма ГОСТ28147-89 содержит
32 раунда

48. Метод шифрования, в котором коды символов открытого текста складываются с элементами случайной или псевдослучайной последовательности называется
Гаммированием

49. Метод защиты информации, который заключается в разработке и реализации в процессе функционирования системы комплексов и мероприятий, создающих такие условия обработки информации, при которых минимизируется риск несанкционированного доступа называется
Регламентацией

50. Значение хэш-функции, в которой используется секретная информация (ключ), называется
Кодом аутентификации сообщения

51. Последовательность операций преобразований одного раунда шифрования алгоритма Rijndael
ByteSub, ShiftRowse, MixColumns

52. Канал утечки информации основанный на перехвате побочных электромагнитных излучений и наводок относится к
Косвенным каналам

53. Принуждение, как метод защиты информации реализуется
Законодательными средствами защиты

54. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена это

Конфиденциальность

55. Шифр Вижинера является
Шифром сложной замены

56. Фактическая длина ключа шифрования алгоритма 3DES составляет
112 бит

57. Режим применения блочного шифра, при котором шифрование текущего блока зависит от текущего и всех предыдущих блоков, причем если последний блок данных не кратен размеру блока криптоалгоритма, необходимо его дополнения до полной длины:
CBC

58. Криптографическая система, в которой один ключ используется для шифрования, а другой (отличный от первого) - для расшифрования, называется
Криптосистемой с открытым ключом

59. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой:
Апеллируемость

60. Функционирование DES в режиме OFB позволяет получить
Криптографическую псевдослучайную последовательность

61. Размер блока алгоритма шифрования ГОСТ 28147-89 составляет
64 бита

62. Цикл шифрования алгоритма ГОСТ 28147-89 в режиме выработки имитовставки содержит
16 раундов

63. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты системы от заданного множества угроз называется:
Политикой безопасности

64. Линейная рекуррентная последовательность является
Некриптографической псевдослучайной последовательностью

65. Преобразование, выполняемое в шифре Rijndael, при котором каждый столбец исходной матрицы слева умножается на постоянную матрицу-циркулянт, называется
    MixColumns

66. «Маски» вирусов используются
    для поиска известных вирусов

67. Ip-адрес имеет длину
    4 байта

68. Security updates (обновления безопасности) необходимы
    для устранения обнаруженных недочетов в установленном ПО в операционных системах, установки патчей для предотвращения возможности эксплуатации уязвимостей, для поддержания внутренней самозащиты программ

69. Алгоритм DES использует длину блока:
    64 бит

70. Алгоритм DES использует длину ключа
    56 бит

71. Алгоритм Диффи-Хеллмана используется для
    открытого распределения ключей

72. Алгоритм Диффи-Хеллмана позволяет
    использовать незащищенный от прослушивания, но защищённый от подмены, канал связи

73. Алгоритм шифрования SHA предназначен для использования совместно с алгоритмом цифровой подписи
    DSA

74. Объект «А» заявляет, что он не посылал сообщение объекту «Б», хотя на самом деле он все-таки посылал:
    отказ (ренегатство)

75. Антивирус – это программа, которая
    удаляет некоторые категории вредоносных программ, достигая успеха менее чем в 100 процентах случаев

76. Аспектами информационной безопасности являются

конфиденциальность, доступность, целостность

77. Аудит информационной безопасности должен включать в себя
анализ информационных рисков с целью оценки вероятно ущерба и инструментальной проверки защищенности для определения возможности реализации угроз

78. Безопасность данных в информационной базе обеспечивается
конфиденциальностью, целостностью и доступностью информации

79. Абонент «А» изменяет сообщение и утверждает, что данное (измененное) сообщение послал ему абонент «Б»
модификация (переделка)

80. Абонент «А» формирует сообщение и утверждает, что данное (измененное) сообщение послал ему абонент «Б»
подделка

81. Более усовершенствованный вид мнемокодов
автокоды

82. В каком году был представлен алгоритм Диффи-Хелмана:
1975г

83. В каком году и где был разработан алгоритм SHA
1993 году в США

84. В версиях MS OFFICE 2007\2010 компания MICROSOFT использует алгоритм шифрования
AES с 128-битным ключом

85. В процедуре постановки подписи используется
секретный ключ отправителя сообщения

86. В процедуре проверки подписи используется
открытый ключ отправителя

87. В процедуре формирования подписи используется
секретный ключ отправителя

88. Абонент «А» только что прислал вам по ICQ ссылку на *.EXE файл в интернете, предложил запустить его и вышел из сети, так что вы не можете уточнить детали. Правильные действия:

никогда не открою ссылку, даже если она от друга

89. Вид злоумышленного действия, если абонент С повторяет ранее переданный документ, который абонент А посылал абоненту В.

повтор

90. Абонент «В» перехватывает сообщения между абонентом «А» и абонентом «Б» с целью их скрытой модификации:

активный перехват

91. Абонент «В» посылает абоненту «Б» сообщение от имени абонента «А»

Маскировка (имитация)

92. Возможность использовать одинаковые имена для методов входящих различные классы называется:

полиморфизм

93. Возможные последствия BOTNET-инфекции:

заражение boot-секторов дисков, могут привести к полной потере всей информации, хранящейся на диске

94. Вы получаете email от вашего банка с просьбой в течение недели подтвердить ваши последние покупки, перейдя на соответствующую страницу сайта банка. Ваши действия

буду бдительным – уточню в банке подлинность письма, не буду кликать ни по каким ссылкам в письме и проверю свой счет, вручную набрав нужный адрес в адресной строке браузера

95. Выберите вид антивирусных программ, перехватывающих «вирусо-опасные» ситуации и сообщающих об этом пользователю

блокировщик

96. Выберите из списка пароль, который наиболее точно соответствует требованиям стандарта

1#derk!

97. Невыполнение какого из следующих требований политики безопасности может наибольшим образом повысить существующие в системе информационные риски

регулярное обновление антивирусных баз

98. Для «сжатия» произвольного сообщения служат

ХЭШ-функции

99. Для защиты системы шифрованной связи от навязывания ложных данных используется
имитозащита

1. Для контроля целостности передаваемых по сетям данных используется
электронная цифровая подпись

2. Для проведения анализа информационных рисков необходимо
построение полной модели информационной системы с точки зрения информационной безопасности

3. Для проверки подписи необходимо использовать
оба ключа – секретный и открытый

4. Для чего используется алгоритм Диффи-Хеллмана
для получения общего секретного ключа при общении через незащищенный канал связи

5. Доступность информации гарантирует
получение требуемой информации за определенное время

6. Европейские критерии аспектов информационной безопасности
конфиденциальность, целостность, доступность

7. Загрузочные вирусы характеризуются тем, что:
поражают загрузочные сектора дисков

8. Злоумышленные действия отправителя заявляющего, что он не посылал сообщение
отказ (ренегатство)

9. Идентификация и аутентификация применяются
для ограничения доступа случайных и незаконных субъектов к информационной системе

10. Имитацией сообщения является
маскировка

11. Информационная безопасность характеризует защищенность
информации и поддерживающей ее инфраструктуру

12. К группе каналов утечки информации, в которой основным средством является аппаратура, относятся

подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации

13. К непреднамеренным угрозам относятся
ошибки в разработке программных средств КС

14. К основным программно-техническим мерам относятся
аутентификация пользователя и установление его идентичности, доступ к данным, целостность данных, протоколирование и аудит, защита коммуникаций между клиентом и сервером

15. К причинам случайных воздействий при эксплуатации не относится
преднамеренный взлом

16. К умышленным угрозам относятся
несанкционированные действия обслуживающего персонала КС вследствие ослабления политики безопасности администратором

17. Наука о математических методах обеспечения конфиденциальности и аутентичности, целостности и подлинности авторства информации
криптография

18. В политике безопасности не рассматривается
анализ экономических рисков

19. Чтобы уменьшить подверженность ПК воздействию на него вредоносного кода
работать под учетной записью с ограниченными правами

20. Электронная подпись шифруется
с помощью специальной программы создаются два ключа: закрытый и публичный

21. Не является группой компонентов автоматизированных информационных систем
среда – период действия, автономность, языковые группы

22. Длина ключа недосягаемая для всех известных алгоритмов взлома:
768 бит

23. В основе DES и ГОСТ 28147-89 лежит схема шифрования
сеть Фейстеля

24. Основной недостаток современных антивирусов
    зависимость от вирусных сигнатур незрелость эвристических методов детекции

25. Действия при назначении прав доступа для нового пользователя
    ознакомление и документальная фиксация назначенных пользователю прав доступа

26. Наиболее точное определение компьютерного вируса
    программа, воспроизводящаяся присоединением части своего кода к обычным файлам с целью распространения и преднамеренного причинения цщерба аппаратному, или программному обеспечению ПК, или файлам

27. Программное обеспечение не доступное в операционной среде
    средства защиты, системные утилиты, системные редакторы, средства разработки

28. Результат шифрования слова "кот" шифром цезаря с ключом
    мрф

29. Вид антивирусных программ, основанный на подсчете контрольных сумм для присутствующих на диске файлов системных секторов:
    crc-сканер

30. Вид резервного копирования, занимающий меньше времени
    инкрементное

31. Вид резервного копирования, ускоряющий процесс восстановления:
    дифференциальное

32. Наилучший вариант, описывающий возможные последствия botnet-инфекции:
    ваш пк будет действовать как сервер, подчиняясь удаленным командам хакера

33. Ключ, доступный всем, для проверки цифровой подписи под документом
    открытый

34. Длина ключа, рекомендуемая лабораторией RSA, для менее ценной информации
    768 бит

35. Длина ключа, рекомендуемая лабораторией RSA, для обычных задач

1024 бита

35. Длина ключа, рекомендуемая лабораторией RSA, для особо важных задач
2048 бита

36. Основная задача в должностной инструкции по защите информации для каждого сотрудника
обеспечение информационной безопасности

37. Кейлоггер – это
программа, использующая технику внедрения в ядро операционной системы для сокрытия присутствия в системе и перехватывающий все нажатия клавиш

38. К разграничению доступа пользователей не относится
матрицы установления полномочий

39. Ключ шифра должен определяться только
секретностью ключа

40. Комплекс предупредительных мер по обеспечению информационной безопасности организации – это
политика безопасности в защите сети

41. Конфиденциальность информации гарантирует
доступность информации кругу лиц, для кого она предназначена

42. Косвенными каналами утечки называют
каналы, не связанные с физическим доступом к элементам КС

43. Маскировка – это
имитация

44. Массированная отправка пакетов данных на узлы сети предприятия, с целью их перегрузки и выведения из строя
DOS атаки

45. Информационная безопасность должна обеспечиваться на
законодательном, административном, процедурном, программном, техническом уровне

46. Алгоритм RSA основан на труднорешаемой задаче
факторизации чисел

47. Метод защиты от вирусов
    программный, аппаратный, организационный

48. Наиболее действенным методом защиты от повтора являются
    использование имитовставок и учет входящих сообщений

49. Наиболее известные из хэш-функций
    MD2, MD4, MD5 и SHA

50. Наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу – это
    криптоанализ

51. Может привести к повышению риска повреждения информации в системе при несоблюдении такого минимального требования, как
    регулярное обновление антивирусных баз

52. Организационными мероприятиями предусматривается
    исключение несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным

53. Основной задачей теста на проникновение является
    оценка возможности осуществления атаки из Интернета на информационную систему компании

54. Основные типы вирусов
    программные, загрузочные, макровирусы

55. Основополагающим документом по информационной безопасности в республики Казахстан является
    концепция информационной безопасности республики казахстан до 2016 года

56. Отказ - это
    ренегатство

57. По масштабу вредных воздействий компьютерные вирусы делятся
    на безвредные, неопасные, опасные, очень опасные

58. По среде обитания компьютерные вирусы бывают:
    файловые, загрузочные, макровирусы, сетевые

59. Под защитой информации понимается

совокупность мероприятий, методов и средств, обеспечивающих решение задач по проверке целостности информации и исключении несанкционированного доступа к ресурсам пэвм и хранящимся в ней программам и данным

60. Под информационной безопасностью понимается
защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации

61. Под организацией доступа к ресурсам понимается
весь комплекс мер, который выполняется в процессе эксплуатации кс для предотвращения несанкционированного воздействия на технические и программные средства и информацию

62. Под угрозой безопасности информации в компьютерной системе (кс) понимают
событие или действие, которое может вызвать изменение функционирования кс, связанное с нарушением защищенности обрабатываемой в ней информации

63. Трудно обнаружимые вирусы, не имеющие сигнатур, не содержащие ни одного постоянного участка кода – это
полиморфик-вирусы

64. Политика информационной безопасности в общем случае является
обще-информационным документом

65. Происхождение термина «криптография»:
от слова «тайнопись»

66. Метод надежной передачи информации по открытому каналу связи использует:
стеганографию

67. Для чего используется система Kerberos?
для симметричной аутентификации;

68. Что такое код обнаружения манипуляции с данными MDC?
есть результат действия хэш-функции

69. Наука об обеспечении секретности и / или аутентичности (подлинности) передаваемых сообщений:
криптография

70. Замену символов с открытого текста, соответствующими символами алфавита криптотекста называют:
шифром замены

71. Функции, для которых легко найти функцию прямого отображения и нельзя найти обратное называются:
односторонние функции

72. Системы, где с помощью открытого ключа шифруют ключ блочного криптоалгоритма, а само сообщение шифруют с помощью этого симметричного секретного ключа, называют:
гибридные криптосистемы

73. Процесс применения шифра защищаемой информации называют:
шифрованием

74. Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения:
ключ

75. Процесс наложения по определенному закону гамма-шифра на открытые данные:
гаммирование

76. Шифр – это …
совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с использованием ключей

77. Разрядность 3DES равна:
112 бит

78. При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы называются:
симметричными криптосистемами

79. Линейное шифрование данных, основанное на поточном способе шифрования называется:
гаммированием

80. Криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись, разработанная в 1977 году, называется:

алгоритм шифрования RSA

81. Цифровая подпись - …
небольшое количество дополнительной цифровой информации, передаваемое вместе с подписываемым текстом, по которому можно удостоверится в аутентичности документа

82. Функция, предназначенная для сжатия подписываемого документа до нескольких десятков, или сотен бит называется:
хэш- функцией

83. Алгоритм, предназначенный для использования совместно с алгоритмом цифровой подписи DSA:
SHA

84. Чему равна разрядность блока алгоритма шифрования DES:
64 битам

85. Цель атаки на криптосистему:
нарушение целостности передачи информации абоненту

86. Установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем (передатчиком) называется:
аутентификацией

87. Совокупность действий (инструкций, команд, вычислений), выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата называется:
протоколом

88. Какова разрядность ключа алгоритма шифрования ГОСТ 28147 – 89 (первого российского стандарта шифрования):
256 бит

89. Почему так широко используют циклы Фейштеля в криптографии?
упрощается процесс дешифрования

90. В развитии средств информационных коммуникаций можно выделить несколько этапов:
7

91. Периметр Безопасности это:

граница доверенной вычислительной базы

92. Выполнение каких-либо действий одним пользователем от имени другого пользователя это:
«Маскарад»

93. Метод физического преграждения пути злоумышленнику к защищаемой информации
препятствие

94. Установление подлинности объекта или субъекта по предъявленному им идентификатору
опознание

95. Процедура проверки соответствия некоего лица и его учетной записи в компьютерной системе
аутентификация

96. Инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала
физические средства

97. Средства защиты, определяемые законодательными актами страны,
законодательные средства

98. Средства защиты, определяемые нормами поведения
морально-этические средства

99. Доступ к информации могут получить только легальные пользователи
конфиденциальность

1. Защищаемая информация может быть изменена только законными и имеющими соответствующие полномочия пользователями
целостность

2. Гарантия беспрепятственного доступа к защищаемой информации для законных пользователей является
апеллируемость

3. Деятельность, направленная на обеспечение информационной безопасности, принято называть

защитой информации

4. Механизмы защиты информации, обрабатываемой в распределённых вычислительных системах и сетях
сервисы сетевой безопасности

5. Потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.
угроза

6. Угрозы, возникшие в результате воздействия на АС объективных физических процессов или стихийных природных явлений, не зависящих от человека
ественные угрозы

7. Угрозы, вызваные действием человеческого фактора
искусственные угрозы

8. Угрозы, вызванные халатностью или непреднамеренными ошибками персонала
случайные угрозы

9. Угрозы, вызванные направленной деятельностью злоумышленника
апеллируемость

10. Угрозы, в результате реализации которых, информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней.
угрозы нарушения конфиденциальности информации

11. Злонамеренное искажение информации, обрабатываемой с использованием АС.
угрозы нарушения целостности информации

12. Угрозы, возникающие в тех случаях, когда доступ к некоторому ресурсу АС для легальных пользователей блокируется
нарушение доступности информации

13. Присвоение субъектам доступа уникальных идентификаторов и сравнение таких идентификаторов с перечнем возможных
идентификация

14. Проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности

аутентификация

15. Метод, позволяющий подобрать любой пароль вне зависимости от его сложности
полный перебор

16. Значительная часть используемых на практике паролей представляет собой осмысленные слова или выражения
подбор по словарю

17. Выбор в качестве пароля некой персональной информации, связанной с пользователем
подбор с использованием сведений о пользователе

18. Подбор паролей по словарю за счёт отбраковки заведомо легко паролей
проверка и отбраковка паролей по словарю

19. Срок действия пароля ограничивает промежуток времени, который злоумышленник может затратить на подбор пароля
установка максимального срока действия пароля

20. Предотвращение попытки пользователя незамедлительно сменить новый пароль на предыдущий
установка минимального срока действия пароля

21. Предотвращение повторного использования паролей – возможно, ранее скомпрометированных.
отбраковка по журналу истории паролей

22. Метод разграничения доступа между поименованными субъектами и поименованными объектами
дискреционный

23. Создание и сопровождение ролей и других атрибутов ролевого доступа
административные функции

24. Обслуживание сеансов работы пользователей
вспомогательные функции

25. Получение сведений о текущей конфигурации с учетом отношения наследования
информационные функции

26. Получение информации о правах, приписывающих роли, о правах заданного пользователя, об активных в данный момент сеансах ролях и правах
    необязательные функции

27. Контроль информационных потоков производится посредством
    фильтрации информации

28. Принцип, который требует обеспечения невозможности произвольной модификации данных пользователем
    корректность транзакций

29. Изменение данных, которое может осуществляться только аутентифицированными для выполнения соответствующих действий пользователями
    аутентификация пользователей

30. Процессы, наделенные только теми привилегиями в АС, которые минимально достаточны для их выполнения
    минимизация привилегий

31. Для выполнения критических или необратимых операций требуется участие нескольких независимых пользователей
    разделение обязанностей

32. Создание механизма подотчётности пользователей, которое позволяет отследить моменты нарушения целостности информации
    аудит произошедших событий

33. Реализация оперативного выделения данных, контроль целостности которых является оправданным
    объективный контроль

34. Порядок передачи привилегий, соответствующий организационной структуре предприятия
    управление передачей привилегий

35. Категории защиты информации, которые были представлены для сертификации по требованиям одного из более высоких классов защищённости, но не прошли испытания
    группа D – минимальная защита

36. Группа, характеризующаяся наличием дискреционного управления доступом и регистрации действий субъектов.

группа С - дискреционная защита

37. Система, обеспечивающая мандатное управление доступом с использованием меток безопасности, поддержку модели и политики безопасности
группа В – мандатная защита

38. Дополнительная документация, демонстрирующая, что архитектура и реализация ядра безопасности отвечает требованиям безопасности
Группа А – верифицированная защита

39. Классы соответствующие АС, в которых работает один пользователь, допущенный ко всей информации
III группа – классы 3Б и 3А

40. Классы данной группы соответствующие АС, в которых пользователи имеют одинаковые права доступа ко всей информации
II группа – классы 2Б и 2А

41. Пользователи, не имеющие доступ ко всей информации в АС в данной группе
I группа – классы 1Д, 1Г, 1В, 1Б и 1А

42. Предоставление конкретному пользователю доступа к определённым системным ресурсам
авторизация

43. Аутентификация на основе пароля, переданного по сети в зашифрованном виде, и не обеспечивает защиты от
воспроизведения

43. Аутентификация на основе пароля, переданного по сети в открытом виде, плоха, и не обеспечивает защиты от
перехвата

44. В качестве аутентификатора в сетевой среде могут использоваться
секретный криптографический ключ

45. В число основных принципов архитектурной безопасности входят
эшелонированность обороны

46. В число классов требований доверия безопасности "Общих критериев" входят:

оценка профиля защиты

47. В число классов функциональных требований "Общих критериев" входят
адекватность

48. В число целей политики безопасности верхнего уровня входят
решение сформировать, или пересмотреть комплексную программу безопасности

49. Контроль целостности может использоваться для:
предупреждения нарушений ИБ

50. Политика безопасности организации:
фиксирует правила разграничения доступа

51. Политика безопасности строится на основе:
анализа рисков

52. Протоколирование и аудит могут использоваться для:
обнаружения нарушений

53. "Общие критерии" содержат следующий вид требований:
доверия безопасности

54. Перехват данных является угрозой:
конфиденциальности

55. Уровень безопасности А, согласно "Оранжевой книге", характеризуется:
верифицируемой безопасностью

56. Уровень безопасности В, согласно "Оранжевой книге", характеризуется:
метками безопасности

57. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:
принудительным управлением доступом

58. Устройство управления разграничением доступа
монитор ссылок

59. Риск является функцией:
вероятности реализации угрозы

60. Цифровой сертификат содержит:

секретный ключ удостоверяющего центра

61. Что понимается под информационной безопасностью?
обеспечение информационной независимости

62. Что такое защита информации?
комплекс мероприятий, направленных на обеспечение ИБ

63. Доступ к информации могут получить только легальные пользователи
конфиденциальность

64. Защищаемая информация, которая может быть изменена только законными и имеющими соответствующие полномочия пользователями
целостность

65. Гарантия беспрепятственного доступа к защищаемой информации для законных пользователей
доступность

66. Состояние защищенности национальных интересов от угроз, исходящих со стороны иностранных государств, организаций и граждан;
внешняя безопасность

67. Состояние защищенности от реальных и потенциальных угроз и посягательств военного характера на независимость и территориальную целостность страны;
военная безопасность

67. Состояние защищенности государственных информационных ресурсов, а также прав личности и интересов общества в информационной сфере
информационная безопасность

68. Официально принятая система взглядов и мер по обеспечению защиты конституционных прав личности и граждан
концепция национальной безопасности

69. Состояние защищенности национальных интересов страны от реальных и потенциальных угроз
национальная безопасность

70. Совокупность политических, экономических, социальных и других потребностей от реализации которых зависит способность государства обеспечивать защиту конституционных прав человека и гражданина

национальные интересы

71. Политико-правовая, духовно-нравственная, социальная защищенность жизни
общественная безопасность

72. Личность, ее права и свободы, общество, его материальные и духовные ценности
объекты национальной безопасности

73. Государство, осуществляющее свои полномочия через органы законодательной, исполнительной и судебной ветвей власти, граждане и организации
субъекты национальной безопасности

74. Совокупность условий, процессов и факторов, препятствующих реализации национальных интересов или создающих им опасность
угрозы национальной безопасности

75. Состояние защищенности жизненно важных интересов и прав личности, возникающих в результате антропогенных и иных воздействий на окружающую среду
экологическая безопасность

76. Состояние защищенности национальной экономики от внутренних и внешних условий
экономическая безопасность

77. Система, которая обеспечивает управление доступом к информации, путем авторизации лиц
безопасная система

78. Система, использующая аппаратные и программные средства для обеспечения одновременной обработки информации без нарушения прав доступа
доверенная система

79. Набор законов, правил, процедур и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию
политика безопасности

80. Система, определяющая меру доверия, и показывающая корректность механизмов, отвечающих за реализацию политики безопасности
уровень гарантированности

81. Это совокупность защитных механизмов информационной системы и реализующих политику безопасности
    Доверенная вычислительная

82. Контроль за выполнением субъектами определенных операций над объектами
    Монитор обращений

83. Конкретная реализация монитора обращений, обладающая гарантированной неизменностью
    Ядро безопасности

84. Граница доверенной вычислительной базы
    Периметр безопасности

85. Неизменность информации в процессе ее передачи или хранения
    целостность

86. Свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования
    доступность

87. Обеспечение идентификации субъекта доступа и регистрации его действий
    подотчётность

88. Свойство соответствия предусмотренному поведению или результату
    достоверность

89. Программное обеспечение, посылающее через интернет не санкционированную пользователем информацию
    Spyware

90. ПО передающее детальную информацию рекламодателям о веб-страницах
    Zango

91. Метод физического преграждения пути злоумышленнику к защищаемой информации
    Препятствие

92. Метод защиты информации регулированием использования всех ресурсов
    Управление доступом

93. Метод защиты информации в автоматизированной информационной системе путем ее криптографического закрытия

Маскировка

94. Метод защиты информации, обеспечивающий минимальный несанкционированный доступ к системе
Регламентация

95. Метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки информации
Принуждение

96. Метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные прав
Побуждение

97. Процесс, используемый для распознавания индивидуального пользователя
Аутентификация

98. Проверка разрешения индивидуальному пользователю на получение информации определённого рода
Авторизация

99. Контролируемая информация должна избирательно храниться и защищаться в мере достаточной для отслеживания
Аудит

1. Чтобы компьютерная система работала слаженно, необходимо соблюдение
Гарантии

2. Совокупность законов, норм и правил, регламентирующих порядок обработки, защиты и распространения информации
Политика безопасности

3. Потребность потребителя продуктов информационных технологий в противостоянии множеству угроз безопасности
Задача защиты

4. Совокупность задач защиты, функциональных требований, требований адекватности и их обоснования
Профиль защиты

5. Совокупность задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования

Проект защиты

6. В процедуре проверки подписи используется:
открытый ключ отправителя

7. В процедуре формирования подписи используется
секретный ключ отправителя

8. Абонент «А» только что прислал вам по ICQ ссылку на *.exe файл в Интернете, предложил запустить его и вышел из сети, так что Вы не можете уточнить детали. Правильные действия:
никогда не открою ссылку, даже если она от друга

9. Вид злоумышленного действия, если абонент С повторяет ранее переданный документ, который абонент А посылал абоненту В.
повтор

10. Вид резервного копирования, ускоряющий процесс восстановления:
дифференциальное

11. Наилучший вариант, описывающий возможные последствия botnet-инфекции:
ваш ПК будет действовать как сервер, подчиняясь удаленным командам хакера;

12. Ключ, доступный всем, для проверки цифровой подписи под документом
открытый

13. Выполнение каких-либо действий одним пользователем от имени другого пользователя это:
«Маскарад»

14. Метод физического преграждения пути злоумышленнику к защищаемой информации
препятствие

15. Установление подлинности объекта или субъекта по предъявленному им идентификатору
опознание

16. Процедура проверки соответствия некоего лица и его учетной записи в компьютерной системе
аутентификация

17. Инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала
    физические средства

18. Средства защиты, определяемые законодательными актами страны,
    законодательные средства

19. Средства защиты, определяемые нормами поведения
    морально-этические средства

20. Доступ к информации могут получить только легальные пользователи
    конфиденциальность

21. Защищаемая информация может быть изменена только законными и имеющими соответствующие полномочия пользователями
    целостность

22. Гарантия беспрепятственного доступа к защищаемой информации для законных пользователей является
    апеллируемость

23. Деятельность, направленная на обеспечение информационной безопасности, принято называть
    защитой информации

24. Механизмы защиты информации, обрабатываемой в распределённых вычислительных системах и сетях
    сервисы сетевой безопасности

25. Потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.
    угроза

26. Угрозы, возникшие в результате воздействия на АС объективных физических процессов или стихийных природных явлений, не зависящих от человека
    ественные угрозы

27. Угрозы, вызванные действием человеческого фактора
    искусственные угрозы

28. Угрозы, вызванные халатностью или непреднамеренными ошибками персонала

случайные угрозы

29. Угрозы, вызванные направленной деятельностью злоумышленника
апеллируемость

30. Угрозы, в результате реализации которых, информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней.
угрозы нарушения конфиденциальности информации

31. Злонамеренное искажение информации, обрабатываемой с использованием, АС.
угрозы нарушения целостности информации

32. Угрозы, возникающие в тех случаях, когда доступ к некоторому ресурсу АС для легальных пользователей блокируется
нарушение доступности информации

33. Уровни секретности
совершенно секретно, секретно, конфиденциально, несекретно

34. Метки безопасности отражают -степень секретности
степень секретности и категории, к которой относятся данные

35. Безопасность повторного использования объектов
предохраняет от случайного или преднамеренного извлечения секретной информации из «мусора»

36. Произвольное управление доступом это
добровольное управление доступом

37. Мандатное разграничение доступа это
разграничение доступа по уровням секретности

38. Дискреционное разграничение доступа это
разграничение доступа между поименованными субъектами и поименованными объектами

39. Методы хранения паролей
В зашифрованном, открытом виде, в виде хэш-значения

40. Присвоение субъектам доступа уникальных идентификаторов и сравнение таких идентификаторов с перечнем возможных

идентификация

41. Проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности

аутентификация

42. Метод, позволяющий подобрать любой пароль вне зависимости от его сложности

полный перебор