Основы информационной безопасности

1. Аккаунт – это

1. Компьютерный вирус
2. Учетная запись
3. Шаблон безопасности
4. Криптографический алгоритм

Правильный ответ: Учетная запись

2. Способ, позволяющий нарушителю получить доступ к информации, называют

1. Каналом утечки информации
2. Криптографическим алгоритмом
3. Аутентификацией
4. Идентификацией

Правильный ответ: Каналом утечки информации

3. Подлинность данных означает, что они

1. Не подвергались преднамеренным искажениям
2. Были созданы законными участниками информационного процесса
3. Верны ответы a). Ь), c)
4. Не подвергались случайным искажениям

Правильный ответ: Верны ответы a). Ь), c)

4. Способ преобразования данных, являющийся секретным полностью или частично, или использующий при работе набор секретных параметров, называется

1. Компьютерный вирус
2. Учетная запись
3. Шаблон безопасности
4. Криптографический алгоритм

Правильный ответ: Криптографический алгоритм

5. Понятие «собственник информации» впервые в отечественном законодательстве вводит

1. Закон «О правовой охране программ для ЭВМ и баз данных»
2. Закон «О государственной тайне»
3. Федеральный закон «Об информации, информатизации и защите информации»
4. Закон «Об авторском праве и смежных правах»

Правильный ответ: Закон «О государственной тайне»

6. Антивирус используется для

1. Создания компьютерных вирусов
2. Распространения компьютерных вирусов
3. Удаления компьютерных вирусов
4. Обнаружения компьютерных вирусов

Правильный ответ: Удаления компьютерных вирусов; Обнаружения компьютерных вирусов

7. Учетная запись состоит из

1. Занимаемой должности
2. Пароля сотрудника
3. Имени человека
4. Имени и пароля конкретного человека

Правильный ответ: Имени и пароля конкретного человека

8. Файл, содержащий параметры безопасности, носит название

1. Криптографический алгоритм
2. Компьютерный вирус
3. Учетная запись
4. Шаблон безопасности

Правильный ответ: Шаблон безопасности

9. Код аутентификации имеет

1. Переменную длину
2. Кратную длину
3. Программно устанавливаемую длину
4. Фиксированную длину

Правильный ответ: Фиксированную длину

10. Код аутентификации вырабатывается

1. Из данных без использования дополнительных ключей
2. Из данных путем сравнения секретного и открытого ключей
3. Из данных с использованием открытого ключа
4. Из данных с использованием секретного ключа

Правильный ответ: Из данных с использованием секретного ключа

11. Процесс преобразования информации, хранящейся в файле, к виду, при котором уменьшается избыточность в ее представлении, называется

1. Создание файла
2. Редактирование файла
3. Архивация файла
4. Инсталляция файла

Правильный ответ: Архивация файла

12. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к частичному изменению их содержания, называются

1. Искажение
2. Разглашение
3. Разрушение
4. Ознакомление

Правильный ответ: Искажение

13. Ассиметричная схема шифрования основана на использовании

1. Одного открытого ключа
2. Открытого и секретного ключей
3. Двух секретных ключей
4. Одного секретного ключа

Правильный ответ: Открытого и секретного ключей

14. Средство защиты от несанкционированного доступа в локальную сеть называется

1. Кластер
2. Брандмауэр
3. Репликатор
4. Драйвер

Правильный ответ: Брандмауэр

15. Искажение данных приводит к нарушению

1. Целостности информации
2. Конфиденциальности информации
3. Доступности информации
4. Достоверности информации

Правильный ответ: Целостности информации

16. Источники информационных угроз могут преследовать цель

1. Ознакомление с охраняемыми сведениями
2. Верны ответы а). Ь), с)
3. Искажение охраняемых сведений
4. Уничтожение охраняемых сведений

Правильный ответ: Верны ответы а). Ь), с)

17. Среди объектов охраны закон «Об авторском праве и смежных правах» предусматривает

1. Базы данных
2. Сообщения о событиях и фактах, имеющие информационный характер
3. Программы для ЭВМ
4. Официальные документы

Правильный ответ: Программы для ЭВМ

18. Свойство систем быть способными обеспечивать подлинность данных носит название

1. Уязвимость
2. Ассиметричность
3. Аутентичность
4. Уникальность

Правильный ответ: Аутентичность

19. Компьютерный вирус может

1. Закрыть доступ к архивной информации паролем
2. Обеспечить криптографическую защиту
3. Присоединяться к другим программам
4. Создавать свои копии и внедрять их в файлы

Правильный ответ: Закрыть доступ к архивной информации паролем; Присоединяться к другим программам; Создавать свои копии и внедрять их в файлы

20. Цифровая подпись проверяется на основе

1. Сравнения секретного и открытого ключей
2. Секретного ключа
3. Открытого ключа
4. Визуального сравнения ее с оригиналом

Правильный ответ: Открытого ключа

21. Условия создания абсолютно стойкой системы защиты информации от прочтения предложил

1. Д. Мардок
2. Д. Листон
3. П. Шнайдер
4. К. Шеннон

Правильный ответ: К. Шеннон

22. DES-это

1. Антивирусная программа
2. Стандарт шифрования данных
3. Самораспаковывающийся архив
4. Электронная доска объявлений

Правильный ответ: Стандарт шифрования данных

23. Аутентификация – это

1. Закрытие доступа к определенной информации
2. Настройка параметров антивируса
3. Процедура проверки, является ли человек тем, за кого он себя выдал при идентификации
4. Атака на компьютерную систему

Правильный ответ: Процедура проверки, является ли человек тем, за кого он себя выдал при идентификации

24. Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена, называется

1. Фальсификация информации
2. Утечка информации
3. Искажение информации
4. Распространение информации

Правильный ответ: Утечка информации

25. Процесс преобразования открытых данных в зашифрованные при помощи шифра называется

1. Идентификация
2. Аутентификация
3. Дешифрование
4. Шифрование

Правильный ответ: Шифрование

26. Основой для формирования государственной политики в сфере информации является

1. Сертификация средств защиты информации
2. Использование зарубежного опыта
3. Доктрина информационной безопасности РФ
4. Изучение технологий компьютерных преступлений

Правильный ответ: Доктрина информационной безопасности РФ

27. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним, называются

1. Разрушение
2. Ознакомление
3. Разглашение
4. Искажение

Правильный ответ: Разглашение

28. Неправомерное овладение конфиденциальной информацией возможно

1. За счет разглашения ее источниками сведений
2. За счет утечки информации через технические средства
3. За счет несанкционированного доступа к охраняемым сведениям
4. Верны ответы a). b), c)

Правильный ответ: За счет утечки информации через технические средства

29. Фальсификация данных приводит к нарушению

1. Достоверности информации
2. Целостности информации
3. Доступности информации
4. Конфиденциальности информации

Правильный ответ: Достоверности информации

30. Для достоверной идентификации автора документа используется

1. Индивидуальный бланк
2. Личная печать
3. Цифровая подпись
4. Аналоговая подпись

Правильный ответ: Цифровая подпись

31. Потенциально возможное происшествие, неважно, преднамеренное или нет. которое может оказать нежелательное воздействие на ИС, а также на информацию, хранящуюся в ней, называется

1. Угроза целостности
2. Угроза безопасности
3. Угроза отказа в обслуживании
4. Угроза раскрытия

Правильный ответ: Угроза безопасности

32. Процедура опознавания человека объектом информатизации называется

1. Дешифрование
2. Шифрование
3. Квитирование
4. Идентификация

Правильный ответ: Идентификация