

Информационная безопасность

ТЕСТЫ С ОТВЕТАМИ

Тесты по теме - Информационная безопасность (защита информации) с ответами

Правильный вариант ответа отмечен знаком +

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- + Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
- + Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

- + Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

- + несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

- + Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- + Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

- + Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
- + органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

- + Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компания

- Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:

- + Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

- + Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

- + Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

- + Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
- + Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- + Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- + Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
- + Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелегального ПО
- + Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- + Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
- + Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризующаяся:

- + Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

- + Целостность
- Доступность
- Актуальности

23) Угроза информационной системе (компьютерной сети) – это:

- + Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной
- Правовой
- + Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:

- + Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

- + Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

- + Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- + Аудит, анализ уязвимостей, риск-ситуаций