Модуль 4. Тест для зачета Анкета для опроса пользователей СКЗИ

*Заполняется персонально пользователем СКЗИ*

ФИО

*Для корректного заполнения просьба отметить один или несколько вариантов ответа*

1. Кто является субъектами информационных отношений?  
   a) Только пользователи информационных систем  
   b) Только владельцы информации  
   c) Люди или организации, взаимодействующие с информацией
2. В интересах субъектов информационных отношений лежит:  
   a) Только обеспечение конфиденциальности информации  
   b) Обеспечение конфиденциальности, целостности и доступности информации  
   c) Только обеспечение доступности информации
3. Что означает конфиденциальность информации?  
   a) Защищенность от несанкционированного раскрытия или доступа третьих лиц  
   b) Защищенность от несанкционированного изменения или уничтожения  
   c) Доступность для авторизованных пользователей в нужное время и место
4. Что означает целостность информации?  
   a) Защищенность от несанкционированного раскрытия или доступа третьих лиц  
   b) Защищенность от несанкционированного изменения или уничтожения  
   c) Доступность для авторизованных пользователей в нужное время и место
5. Что означает доступность информации?  
   a) Защищенность от несанкционированного раскрытия или доступа третьих лиц  
   b) Защищенность от несанкционированного изменения или уничтожения  
   c) Доступность для авторизованных пользователей в нужное время и место
6. Что такое несанкционированный доступ к информации?  
   a) НСД – Объекты защиты информационных систем  
   b) НСД – Цели защиты информационных систем  
   c) Несанкционированный доступ – угроза безопасности информации
7. Какие источники угроз безопасности информации могут быть внутренними?  
   a) Хакерские атаки  
   b) Ошибки сотрудников  
   c) Физические угрозы  
   d) Спам и фишинг
8. Какие меры защиты используются для противодействия угрозам безопасности информации?  
   a) Организационные, технические и физические  
   b) Политические, экономические и социальные  
   c) Административные, финансовые и операционные  
   d) Физические, технические и межличностные
9. Какие меры включает в себя организационная защита информации?  
   a) Разработка политики безопасности, проведение аудитов безопасности, обучение сотрудников  
   b) Установление правил доступа и управление аутентификацией пользователей  
   c) Использование фаерволлов и антивирусного ПО  
   d) Физическая защита серверных помещений и системы видеонаблюдения
10. Какие меры включает в себя техническая защита информации?  
    a) Использование фаерволлов и антивирусного ПО  
    b) Разработка политики безопасности и проведение аудитов безопасности  
    c) Физическая защита серверных помещений и системы видеонаблюдения  
    d) Обучение сотрудников и установление правил доступа
11. Какие меры включает в себя физическая защита информации?  
    a) Физическая защита серверных помещений, системы видеонаблюдения, контроль доступа и биометрическая идентификация  
    b) Разработка политики безопасности и проведение аудитов безопасности  
    c) Использование фаерволлов и антивирусного ПО  
    d) Обучение сотрудников и установление правил доступа
12. Какие достоинства организационных мерозащиты информации?  
    a) Они формируют правильную культуру безопасности в организации и являются основой для обеспечения безопасности информации  
    b) Они блокируют и обнаруживают атаки  
    c) Они защищают от новых и неизвестных угроз  
    d) Они предотвращают проникновение злоумышленников при использовании социальной инженерии
13. Какой принцип предполагает предоставление доступа к системам и данным только необходимым пользователям с минимальными правами?  
    a) Принцип наименьшего привилегирования  
    b) Принцип защиты в глубину  
    c) Принцип постоянного мониторинга и обновления  
    d) Принцип обучения и осведомления пользователей
14. Какой принцип предполагает использование различных уровней и слоев защиты для предотвращения или затруднения проникновения злоумышленников?  
    a) Принцип наименьшего привилегирования  
    b) Принцип защиты в глубину  
    c) Принцип постоянного мониторинга и обновления  
    d) Принцип обучения и осведомления пользователей.
15. Какие требования устанавливает закон к качеству информации?  
    a) Точность и достоверность  
    b) Обязательность наличия электронных копий информации  
    c) Применение новейших информационных технологий
16. Какие права гарантирует закон в отношении доступа к информации?  
    a) Право на получение информации из открытых источников  
    b) Право на получение информации только с разрешения обладателя информации  
    c) Право на получение информации только для государственных органов
17. Какой приказ устанавливает основные положения и требования по безопасному использованию средств криптографической защиты информации с ограниченным доступом?  
    a) Приказ ФАПСИ от 13.06.2001 № 152  
    b) Приказ ФАПСИ от 13.06.2001 № 153  
    c) Приказ ФАПСИ от 13.06.2001 № 154  
    d) Приказ ФАПСИ от 13.06.2001 № 155
18. Что рассматривается в инструкции по безопасному использованию средств криптографической защиты информации с ограниченным доступом?  
    a) Риски использования электронной подписи (ЭП)  
    b) Требования к процедурам создания и хранения резервных копий ключей  
    c) Общие принципы и задачи безопасности при использовании средств криптографической защиты информации с ограниченным доступом
19. Какие действия регламентируются в инструкции по управлению своими сертификатами?  
    a) Отзыв, приостановка и возобновление действия сертификатов  
    b) Создание и хранение резервных копий ключей  
    c) Требования к контролю доступа к сертификационным центрам
20. Что включает процесс установки и настройки СКЗИ КриптоПро CSP?  
    a) Установку необходимых компонентов и настройку параметров работы СКЗИ  
    b) Хранение ключевых носителей и кодов доступа  
    c) Проверку срока действия сертификата ЭП  
    d) Соблюдение требований безопасности и инструкций по использованию СКЗИ
21. Что следует обеспечивать при работе с СКЗИ?  
    a) Безопасное хранение ключевых носителей и кодов доступа  
    b) Установку необходимых компонентов и настройку параметров работы СКЗИ  
    c) Проверку срока действия сертификата ЭП  
    d) Соблюдение требований безопасности и инструкций по использованию СКЗИ
22. Что не рекомендуется делать при хранении ключевых носителей и кодов доступа?  
    a) Хранить их вместе  
    b) Хранить их в недостаточно защищенном месте  
    c) Контролировать и учет использования СКЗИ  
    d) Вести журналы использования и аудита
23. Что такое квалифицированная электронная подпись?  
    a) Электронная подпись, которая выполняет требования закона и использует квалифицированный сертификат ключа проверки электронной подписи.  
    b) Электронная подпись, которая не соответствует требованиям закона.  
    c) Электронная подпись, выполняющая усиленные криптографические алгоритмы.
24. Что такое сертификат ключа проверки электронной подписи?  
    a) Электронный документ, выдаваемый удостоверяющим центром, подтверждающий соответствие открытого ключа электронной подписи владельца сертификата и его личности.  
    b) Электронный документ, используемый для шифрования электронной подписи.  
    c) Электронный документ, выдаваемый государственными органами для подтверждения личности человека.
25. Какое значение имеет квалифицированная электронная подпись в России?  
    a) Она признается равноценной собственноручной подписи в письменных документах.  
    b) Она не имеет особого значения по сравнению с другими видами электронных подписей.  
    c) Она используется только для ограниченного числа документов.

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата

Результаты проверки

Всего ответов (кол-во)

Правильных ответов (кол-во) (зачтено/не зачтено)

Проверил

ФИО, подпись