Тест

1. Что такое информационная безопасность?
   a) Защита информации от несанкционированного доступа
   b) Процесс оптимизации работы с информацией
   c) Защита различных информационных систем от потерь и разрушений
   d) Все вышеперечисленное

2. Какое из следующих определений относится к понятию "информация"?
   a) Набор данных, который не имеет смысла
   b) Любые данные, которые можно хранить
   c) Данные, обработанные и имеющие значение для пользователя
   d) Объект, который передается по сети

3. Термин "актив" в информационной безопасности означает:
   a) Ценность объектов, относящихся к информации
   b) Пользователи, имеющие доступ к информации
   c) Уязвимости информационных систем
   d) Метод защиты информации

4. Какой механизм защиты используется для контроля доступа к информации?
   a) Аутентификация
   b) Шифрование
   c) Резервное копирование
   d) Защита от вирусов

5. Какой из перечисленных методов считается техническим механизмом защиты информации?
   a) Политика безопасности
   b) Файрвол
   c) Обучение персонала
   d) Анализ угроз

6. Какой критерий используется для оценки уровня информационной безопасности?
   a) Эффективность использования ресурсов
   b) Конфиденциальность информации
   c) Доступность зданий
   d) Скорость обработки данных

7. Что означает термин "доступность" в контексте информационной безопасности?
   a) Защита данных от потерь
   b) Возможность доступа пользователей к информации, когда это необходимо
   c) Ограничение доступа к информации
   d) Способ защиты информации от копирования

8. Какой из методов не используется для контроля доступа?
   a) Пароли
   b) Распознавание запахов
   c) Отпечатки пальцев
   d) Смарт-карты

9. Какой подход реализует контроль доступа на основе ролей?
   a) DAC (Discretionary Access Control)
   b) MAC (Mandatory Access Control)
   c) RBAC (Role-Based Access Control)
   d) ABAC (Attribute-Based Access Control)

10. Что такое защищаемое помещение в контексте информационной безопасности?
   a) Офис, где работают только юристы
   b) Помещение с ограниченным физическим доступом для защиты информации
   c) Комната для хранения серверов
   d) Технический кабинет с копировальной техникой

11. Что такое угроза в контексте информационной безопасности?
   a) Любое действие, нарушающее работу системы
   b) Риск повреждения данных
   c) Потенциальное событие, которое может нанести ущерб информации или активам
   d) Защитные меры для информации

12. Какой из следующих вариантов не относится к уязвимостям информационных систем?

a) Неправильные настройки оборудования

b) Отсутствие резервного копирования

c) Разработка программного обеспечения

d) Человеческая ошибка

13. Как называется структура, фиксирующая трудности, связанные с угрозами?

a) Модель угроз

b) Система анализа

c) Программа защиты

d) Статистика инцидентов

14. Какую роль играют факторы риска в пролонгации угроз?

a) Они полностью блокируют угрозы

b) Создают новые возможности для уязвимостей

c) Увеличивают вероятность реализации угроз

d) Низконаучные предположения

15. Что такое уязвимость в информационной безопасности?

a) Эффективность методов защиты

b) Слабость в системе, позволяющая атакующим действовать

c) Защита от пожара

d) Эффективная политика безопасности

16. Какой из следующих факторов считается субъективным внутренним фактором?

a) Программное обеспечение

b) Уровень подготовки сотрудников

c) Технические средства защиты

d) Внешние угрозы

17. Объективные внешние факторы включают:

a) Экономическую ситуацию и природные катастрофы

b) Отсутствие знаний сотрудников

c) Устаревшие системы защиты

d) Внутренние конфликты

18. Что такое субъективные внешние факторы?

a) Политическая ситуация в стране

b) Мнения и оценка внешних экспертов

c) Разработка новых технологий

d) Кибератаки на систему

19. Какой из перечисленных факторов не является внешним?

a) Действия конкурентов

b) Техническое обеспечение компании

c) Маркетинговая стратегия

d) Изменение законодательства

20. Что представляет собой обобщенная модель способов овладения информацией?

a) Стратегия кибербезопасности

b) Комбинация методов и техник, позволяющих получить доступ к конфиденциальным данным

c) Политика защиты конфиденциальной информации

d) Программа обучения сотрудников

21. Какой тип шифрования обеспечивает высокий уровень безопасности данных?

a) Симметричное шифрование

b) Ассимметричное шифрование

c) Статистическое шифрование

d) Полевое шифрование

22. Что такое фишинг?

a) Техника взлома компьютера

b) Защищенный способ передачи данных

c) Метод обмана для получения конфиденциальной информации

d) Способ физического проникновения в серверное помещение

23. Что включает в себя план реагирования на инциденты?

a) Описание всех сотрудников

b) Порядок действий при возникновении инцидента

c) Список всех программных продуктов

d) Востребованные лицензионные соглашения

24. Какой из следующих методов не относится к управлению рисками?

a) Избежание рисков

b) Применение нецелевых технологий

c) Снижение рисков

d) Передача рисков

25. Какой метод обучения наиболее эффективен для повышения уровня безопасности в организации?

a) Регулярные тренинги по безопасности

b) Печатные инструкции

c) Поддержка технической документации

d) Стажировки в других компаниях

26. Что такое аудит безопасности?

a) Оценка систем управления безопасностью информационных ресурсов

b) Опрос сотрудников о их знаниях в безопасности

c) Процесс создания новых программ безопасности

d) Тестирование программного обеспечения

27. Какой элемент не является частью системы управления безопасностью?

a) Политики безопасности

b) Процедуры обеспечения безопасности

c) Личное мнение сотрудников о безопасности

d) Технические контроли

28. Что такое двойное шифрование?

a) Использование двух различных алгоритмов шифрования для одной и той же информации

b) Процесс разблокировки зашифрованной информации

c) Применение защиты к физическим документам

d) Анализ уязвимостей

29. Что такое средство защиты информации?

a) Любой документ, содержащий информацию о безопасности

b) Механизм или метод, который защищает информацию от угроз

c) Пользователь, контролирующий доступ к информации

d) Устройство для хранения данных

30. Что включается в политику безопасности информации?

a) Заголовки документов

b) Стандартные операции в компании

c) Правила и процедуры защиты информации

d) Описание программного обеспечения

31. Какой из следующих методов защиты не является физическим?

a) Шифрование данных

b) Замки на дверях

c) Системы видеонаблюдения

d) Препятствия к доступу

32. Что такое бэкдор?

a) Программное обеспечение для резервного копирования

b) Легитимный механизм доступа к системе

c) Тайный способ обхода систем защиты

d) Методы восстановления данных

33. Какой тип антивирусного программного обеспечения обеспечивает максимальную защищенность?

a) Проактивное антивирусное ПО

b) Реактивное антивирусное ПО

c) Периодическое тестирование

d) Системы резервирования данных

34. Какой из следующих типов угроз не рассматривается как административный?

a) Утечка персональных данных

b) Кибератака

c) Недостаток обучения сотрудников

d) Неправильные организационные решения

35. Наиболее распространенный способ защиты данных при передаче информации по сети?

a) Использование протокола HTTPS

b) Шифрование на стороне клиента

c) Автоматическая проверка данных

d) Программное обеспечение для защиты

36. Что такое несанкционированный доступ?

a) Доступ к системе людьми, у которых нет на это прав

b) Доступ только для гостей

c) Контроль за пользователями системы

d) Проверка прав доступа

37. Какое действие не защищает информацию?

a) Регулярное резервное копирование

b) Использование многофакторной аутентификации

c) Игнорирование обновлений ПО

d) Обучение сотрудников

38. Что необходимо делать для защиты информации от внутреннего воздействия?

a) Установить фаервол

b) Проводить тренинги для сотрудников

c) улучшить систему очищения

d) Изолировать сети

39. Какие факторы могут воздействовать на информацию?

a) Только внутренние факторы

b) Только внешние факторы

c) Только субъективные факторы

d) Все перечисленные факторы

40. Что такое инцидент безопасности?

a) Запланированное событие

b) Событие, которое вызывает нарушения безопасности

c) Процесс обновления системы

d) Проведение аудита безопасности