|  |
| --- |
|  |
| Экзаменационный билет № 1 |
| 1. TUN и TAP виртуальные интерфейсы. Применение для защиты информации.   **TUN интерфейсы:** работают на уровне IP-пакетов (сетевой уровень OSI), имитируя сетевой интерфейс и маршрутизируя IP-пакеты между узлами.  **TAP интерфейсы:** работают на уровне Ethernet-кадров (канальный уровень OSI), имитируя Ethernet-интерфейс и пересылая кадры между сетями.  **Применение для защиты информации:**   1. **VPN:** создают защищенные туннели для передачи данных, предотвращая их перехват. 2. **Изоляция трафика:** сегментируют сети для повышения безопасности, ограничивая доступ. 3. **Мониторинг и анализ трафика:** обеспечивают безопасный анализ и фильтрацию данных. 4. **Снижение риска атак:** минимизируют возможность атак типа "человек посередине".   Таким образом, TUN и TAP интерфейсы играют ключевую роль в создании безопасных и изолированных сетевых сред.   1. Классификация информационных систем как объектов информатизации.   Информационные системы (ИС) можно классифицировать по различным критериям:   1. **По уровню управления:**    * **Операционные:** обеспечивают выполнение повседневных операций (например, системы управления складом).    * **Тактические:** помогают в среднесрочном планировании и управлении (например, системы управления производством).    * **Стратегические:** поддерживают долгосрочное планирование и принятие решений (например, системы бизнес-анализа). 2. **По функциональному назначению:**    * **Управленческие:** автоматизируют процессы управления (например, ERP-системы).    * **Производственные:** управляют производственными процессами (например, системы SCADA).    * **Информационно-аналитические:** собирают и анализируют данные для принятия решений (например, системы BI). 3. **По степени интеграции:**    * **Интегрированные:** объединяют несколько функциональных областей в одной системе (например, комплексные ERP-системы).    * **Локальные:** предназначены для решения отдельных задач (например, бухгалтерские программы). 4. **По архитектуре:**    * **Централизованные:** все компоненты и данные находятся в одном месте (например, мейнфреймы).    * **Распределенные:** компоненты и данные распределены по разным узлам сети (например, облачные системы). 5. **По сфере применения:**    * **Корпоративные:** используются в крупных организациях для управления бизнес-процессами.    * **Специализированные:** разрабатываются для решения специфических задач (например, медицинские ИС).    * **Общие:** применяются в различных областях (например, офисные приложения). |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 2 |
| 1. Средства обеспечения конфиденциальности в ОС.   **Средства обеспечения конфиденциальности в ОС**   1. **Мандатное управление доступом (MAC):**    * Регулирует доступ к ресурсам на основе уровней безопасности и категорий, назначаемых администратором. 2. **Дискреционное управление доступом (DAC):**    * Позволяет владельцам ресурсов управлять доступом к ним, устанавливая права для других пользователей. 3. **Контроль доступа на основе ролей (RBAC):**    * Управляет доступом, назначая пользователям роли с определёнными правами. 4. **Шифрование данных:**    * Применяется для защиты данных на дисках (например, BitLocker, LUKS) и при передаче (например, TLS). 5. **Аудит и логирование:**    * Отслеживает и регистрирует события и действия пользователей, помогая выявлять и предотвращать несанкционированный доступ. 6. **Изоляция процессов:**    * Обеспечивает выполнение процессов в отдельных пространствах памяти, предотвращая несанкционированный доступ между ними (например, контейнеризация и виртуализация). 7. **Механизмы аутентификации:**    * Используют пароли, смарт-карты, биометрические данные для подтверждения личности пользователя. 8. **Многофакторная аутентификация (MFA):**    * Требует подтверждения личности с использованием нескольких факторов (например, пароль + SMS-код). 9. **Средства управления правами и политиками:**    * Определяют и контролируют права доступа пользователей и приложений к системным ресурсам (например, AppArmor, SELinux). 10. Порядок проектирования системы защиты информации информационной системы.    **Анализ требований и оценка рисков:**   * Определение требований безопасности на основе законодательства, стандартов и внутренних политик. * Идентификация угроз и уязвимостей, оценка возможных рисков и их воздействия на систему.    **Определение политики безопасности:**   * Разработка общей политики безопасности, включающей цели, принципы и правила обеспечения безопасности информации.    **Проектирование архитектуры защиты:**   * Определение зон безопасности и сегментация сети. * Выбор и планирование внедрения защитных механизмов (фаерволы, системы обнаружения вторжений, VPN, и т.д.).    **Разработка плана управления доступом:**   * Определение методов аутентификации и авторизации пользователей. * Разработка правил и процедур управления доступом на основе принципа минимальных привилегий.    **Внедрение криптографических средств:**   * Выбор и реализация методов шифрования данных при хранении и передаче. * Организация управления ключами и их безопасного хранения.    **Проектирование системы мониторинга и аудита:**   * Определение средств и методов мониторинга активности пользователей и систем. * Внедрение журналирования событий безопасности и анализа логов.    **Разработка плана реагирования на инциденты:**   * Определение процедур обнаружения, анализа и реагирования на инциденты безопасности. * Создание команды реагирования на инциденты (CSIRT) и обучение персонала.    **Тестирование и оценка системы безопасности:**   * Проведение тестов на проникновение и уязвимость для проверки эффективности внедренных мер. * Оценка соответствия системы защиты установленным требованиям и стандартам.    **Документирование системы защиты:**   * Составление документации по всем аспектам системы защиты: политики, процедуры, инструкции и отчеты.    **Постоянный мониторинг и обновление:**   * Регулярный мониторинг состояния безопасности и обновление системы защиты в ответ на новые угрозы и изменения в системе. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 3 |
| 1. Протоколы защиты передаваемой по сети информации в ОС Window   **Протоколы защиты передаваемой по сети информации в ОС Windows**   1. **IPsec (Internet Protocol Security):**    * Обеспечивает конфиденциальность, целостность и аутентификацию IP-трафика.    * Использует шифрование и проверку подлинности на уровне сетевого протокола.    * Применяется для создания VPN и защищенных соединений между хостами или сетями. 2. **TLS (Transport Layer Security):**    * Обеспечивает защиту данных при передаче между клиентом и сервером.    * Используется в протоколах HTTPS, SMTPS, FTPS и других.    * Обеспечивает аутентификацию серверов и клиентов, шифрование данных и их целостность. 3. **SSL (Secure Sockets Layer):**    * Предшественник TLS, обеспечивает схожие функции защиты данных.    * Хотя устарел, все еще используется в некоторых системах. 4. **Kerberos:**    * Протокол аутентификации, используемый для безопасного обмена информацией в сетях.    * Использует билеты для предоставления доступов и защиты передаваемых данных.    * Интегрирован в Windows для обеспечения безопасности при аутентификации и авторизации пользователей. 5. **SMB (Server Message Block) с подписыванием и шифрованием:**    * Обеспечивает безопасную передачу файлов и принтеров в сетях Windows.    * Поддерживает цифровое подписывание сообщений для обеспечения целостности данных.    * В версиях SMB 3.0 и выше реализовано шифрование трафика. 6. **RDP (Remote Desktop Protocol):**    * Используется для удаленного доступа к рабочим столам и приложениям.    * Поддерживает шифрование данных и аутентификацию пользователей для защиты передаваемой информации. 7. **L2TP/IPsec (Layer 2 Tunneling Protocol/IPsec):**    * Объединяет возможности L2TP и IPsec для создания защищенных VPN-соединений.    * Обеспечивает шифрование, целостность и аутентификацию данных на уровне туннеля. 8. **HTTPS (HTTP Secure):**    * Обеспечивает безопасную передачу данных в веб-приложениях.    * Использует TLS для шифрования данных между веб-браузером и сервером. 9. Порядок аттестации системы защиты информации информационной системы.    **Подготовительный этап:**   * **Определение объекта аттестации:** Выбор информационной системы (ИС), подлежащей аттестации. * **Назначение ответственных:** Определение лиц или группы, ответственных за проведение аттестации. * **Сбор документации:** Сбор всех необходимых документов и данных о системе (техническая документация, схемы, политика безопасности и т.д.).    **Предварительный анализ:**   * **Оценка текущего состояния:** Анализ существующих мер защиты и их соответствие нормативным требованиям. * **Выявление угроз и уязвимостей:** Определение потенциальных угроз и уязвимостей ИС.    **Разработка программы и методики аттестации:**   * **Программа аттестации:** Определение целей, задач, этапов и сроков проведения аттестации. * **Методика аттестации:** Определение методов и средств, которые будут использоваться для проверки системы защиты.    **Проведение испытаний и проверок:**   * **Технические испытания:** Проведение тестов на проникновение, сканирование уязвимостей и другие технические проверки. * **Анализ соответствия:** Сравнение фактического состояния системы защиты с установленными требованиями и стандартами. * **Документирование результатов:** Фиксация результатов испытаний и проверок.    **Оценка соответствия:**   * **Анализ результатов:** Оценка полученных данных и определение степени соответствия системы защиты требованиям. * **Разработка рекомендаций:** Формулировка рекомендаций по устранению выявленных недостатков и улучшению системы защиты.    **Подготовка отчета об аттестации:**   * **Составление отчета:** Подготовка итогового документа, включающего результаты проверки, выявленные проблемы и рекомендации. * **Согласование отчета:** Представление отчета на рассмотрение и утверждение уполномоченными лицами или органами.    **Утверждение и оформление результатов:**   * **Принятие решения:** Утверждение результатов аттестации и принятие решения о соответствии системы защиты установленным требованиям. * **Оформление сертификата:** Выдача аттестационного сертификата, подтверждающего соответствие системы защиты требованиям.    **Мониторинг и контроль:**   * **Планирование аудитов:** Определение графика регулярных проверок и аудитов системы защиты. * **Постоянный мониторинг:** Осуществление постоянного контроля за состоянием системы защиты и ее соответствием требованиям |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 4 |
| 1. Механизмы контроля целостности данных. Используемые алгоритмы.   **Механизмы контроля целостности данных:**   1. **Контрольные суммы (Checksums):**    * Используются для быстрого обнаружения ошибок в данных при передаче или хранении.    * Простые алгоритмы, такие как CRC (Cyclic Redundancy Check), вычисляют контрольную сумму данных, которая передается вместе с ними. Получатель вычисляет контрольную сумму снова и сравнивает ее с полученной. 2. **Криптографические хеш-функции:**    * Преобразуют данные произвольной длины в фиксированный размер хеш (хеш-сумму).    * Гарантируют, что малейшее изменение в исходных данных приводит к значительному изменению хеш-суммы.    * Обеспечивают устойчивость к коллизиям (случаи, когда разные данные имеют одинаковую хеш-сумму). 3. **Коды аутентификации сообщений (MAC):**    * Используются для проверки целостности и аутентичности данных.    * Создаются с помощью симметричного ключа и хеш-функции, например, HMAC (Hash-based Message Authentication Code). 4. **Цифровые подписи:**    * Используются для проверки целостности и подлинности данных.    * Создаются с помощью асимметричного шифрования (приватный и публичный ключи). Пример: подпись данных с помощью приватного ключа и проверка с помощью публичного. 5. **Механизмы ECC (Error Correction Codes):**    * Обнаруживают и исправляют ошибки в данных.    * Пример: коды Хэмминга, используемые в памяти компьютеров и системах хранения данных.   **Используемые алгоритмы:**   1. **CRC (Cyclic Redundancy Check):**    * Простой и эффективный алгоритм для проверки целостности данных.    * Широко используется в сетевых протоколах и файловых системах. 2. **MD5 (Message Digest Algorithm 5):**    * Вычисляет 128-битную хеш-сумму.    * Считается устаревшим и небезопасным из-за уязвимости к коллизиям.    **SHA-1 (Secure Hash Algorithm 1):**   * Вычисляет 160-битную хеш-сумму. * Устарел и уязвим к коллизиям, но все еще используется в некоторых системах.    **SHA-2 (Secure Hash Algorithm 2):**   * Семейство алгоритмов (SHA-224, SHA-256, SHA-384, SHA-512). * Вычисляют хеш-суммы разной длины (от 224 до 512 бит). * Широко используются и считаются надежными.    **SHA-3 (Secure Hash Algorithm 3):**   * Современный стандарт хеширования, основанный на алгоритме Keccak. * Обеспечивает высокую безопасность и устойчивость к коллизиям.    **HMAC (Hash-based Message Authentication Code):**   * Комбинирует хеш-функции (например, SHA-256) с секретным ключом для создания MAC. * Используется в различных протоколах безопасности (например, TLS, IPsec).    **Digital Signature Algorithm (DSA):**   * Создает цифровые подписи для проверки целостности и подлинности данных. * Основан на асимметричной криптографии.  1. Порядок создания системы защиты информации информационной системы. |
|  **Определение требований безопасности:**   * **Анализ нормативных требований:** Изучение законодательных актов, стандартов и регламентов, применимых к информационной системе. * **Определение внутренних требований:** Разработка внутренних политик безопасности, исходя из специфики организации и её бизнес-процессов.    **Анализ рисков и угроз:**   * **Идентификация активов:** Определение всех компонентов системы, подлежащих защите (данные, оборудование, программное обеспечение). * **Оценка рисков:** Выявление потенциальных угроз и уязвимостей, анализ вероятности их реализации и возможных последствий.    **Разработка политики безопасности:**   * **Общие принципы:** Определение общих принципов и подходов к обеспечению безопасности информации. * **Правила и процедуры:** Разработка конкретных правил и процедур для защиты информации.    **Проектирование системы защиты:**   * **Определение архитектуры защиты:** Разработка архитектуры защиты, включающей зоны безопасности и их взаимодействие. * **Выбор средств защиты:** Подбор технических и программных средств защиты (фаерволы, системы обнаружения вторжений, антивирусы, криптографические средства и т.д.).    **Разработка и внедрение средств защиты:**   * **Технические меры:** Внедрение сетевых фаерволов, систем обнаружения и предотвращения вторжений, антивирусных программ, систем резервного копирования. * **Организационные меры:** Разработка инструкций, проведение обучения персонала по вопросам информационной безопасности. * **Криптографические меры:** Внедрение систем шифрования данных и управления ключами.    **Тестирование и оценка эффективности:**   * **Тестирование безопасности:** Проведение тестов на проникновение, сканирование уязвимостей, проверка работоспособности внедренных средств защиты. * **Аудит безопасности:** Проведение внутреннего или внешнего аудита для оценки соответствия системы защиты установленным требованиям и стандартам.    **Внедрение системы мониторинга и реагирования на инциденты:**   * **Система мониторинга:** Развертывание систем мониторинга безопасности для отслеживания событий и инцидентов. * **План реагирования на инциденты:** Разработка и внедрение плана реагирования на инциденты безопасности, включая процедуры уведомления, расследования и устранения последствий.    **Документирование системы защиты:**   * **Документация:** Составление и поддержание актуальной документации по системе защиты, включающей политики, инструкции, отчеты и журналы. * **Инструкции и регламенты:** Разработка и утверждение инструкций и регламентов для пользователей и администраторов системы.    **Обучение и повышение осведомленности:**   * **Обучение персонала:** Проведение регулярных тренингов и семинаров по вопросам информационной безопасности. * **Проверка знаний:** Проведение тестирования знаний сотрудников по вопросам безопасности.    **Постоянное улучшение и обновление:**   * **Регулярные аудиты и тестирования:** Планирование и проведение регулярных проверок и тестов системы безопасности. * **Анализ и улучшение:** Постоянный анализ состояния безопасности и внедрение улучшений на основе новых угроз и технологий. |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 5 |
| 1. Идентификация и аутентификация в ОС Windows. Понятия идентификации и аутентификации пользователей. Механизмы начального входа в систему   **Идентификация и аутентификация в ОС Windows** Понятия:  1. **Идентификация:**    * Процесс определения личности пользователя, предъявляющего свои учетные данные системе.    * Пример: ввод имени пользователя (username) при входе в систему. 2. **Аутентификация:**    * Процесс проверки подлинности предъявленных учетных данных.    * Пример: проверка пароля, соответствующего введенному имени пользователя.  Механизмы начального входа в систему:  1. **Логин и пароль:**    * **Идентификация:** Пользователь вводит свое имя пользователя.    * **Аутентификация:** Пользователь вводит пароль, который система проверяет на соответствие сохраненному хешу. 2. **Многофакторная аутентификация (MFA):**    * Использует несколько факторов для проверки подлинности:      + **Что-то, что вы знаете:** Пароль или PIN.      + **Что-то, что у вас есть:** Смарт-карта, мобильное устройство с одноразовым паролем (OTP).      + **Что-то, чем вы являетесь:** Биометрические данные (отпечаток пальца, распознавание лица). 3. **Смарт-карты и токены:**    * **Идентификация:** Вставка смарт-карты или USB-токена.    * **Аутентификация:** Ввод PIN-кода, связанного с устройством, для подтверждения личности. 4. **Биометрическая аутентификация:**    * **Идентификация и аутентификация:** Использование биометрических данных, таких как отпечатки пальцев, сканирование радужной оболочки глаза или распознавание лиц. Windows Hello - пример встроенного механизма в Windows 10 и выше. 5. **Керберос (Kerberos):**    * Сетевая система аутентификации, использующая билеты (tickets) для проверки подлинности пользователей и служб.    * **Идентификация:** Пользователь вводит имя пользователя.    * **Аутентификация:** Пользователь вводит пароль, который проверяется на сервере аутентификации (AS). Сервер выдает билет для доступа к ресурсам. 6. **Windows Hello for Business:**    * **Идентификация и аутентификация:** Объединяет биометрию и ключи безопасности для обеспечения безопасного входа без использования пароля.  Механизмы аутентификации в Active Directory:  1. **Active Directory (AD):**    * Центральная служба управления пользователями и ресурсами в сети Windows.    * Обеспечивает централизованное хранение учетных данных и политики безопасности. 2. **LDAP (Lightweight Directory Access Protocol):**    * Протокол доступа к иерархическим директориям, таким как Active Directory.    * Используется для идентификации и аутентификации пользователей. 3. **NTLM (NT LAN Manager):**    * Старый протокол аутентификации, используемый для обратной совместимости.    * **Идентификация:** Ввод имени пользователя.    * **Аутентификация:** Проверка хешированного пароля.  Процесс начального входа в систему:  1. **Ввод учетных данных:**    * Пользователь вводит имя пользователя и пароль на экране входа. 2. **Проверка учетных данных:**    * Локальная система или сервер Active Directory проверяет подлинность пароля, используя один из поддерживаемых механизмов (например, Kerberos, NTLM). 3. **Создание сессии:**    * При успешной аутентификации создается пользовательская сессия, предоставляющая доступ к ресурсам системы. 4. **Применение политик безопасности:**    * Политики безопасности, установленные администратором, применяются к сессии пользователя, включая ограничения доступа и правила использования системы. 5. Классификация информации, распространение и (или) предоставление которой ограничено в соответствии с законодательством Республики Беларусь   В Республике Беларусь существует система классификации информации, которая определяет уровень её конфиденциальности и ограничивает доступ к ней в соответствии с законодательством. Классификация информации включает следующие уровни:   1. **Общедоступная информация:** Информация, которая может быть свободно распространена и доступна для ознакомления широкому кругу лиц. Не подлежит ограничениям в распространении. 2. **Ограниченная информация:** Информация, доступ к которой ограничен по определенным критериям, установленным законодательством. Классифицируется на подуровни в зависимости от степени конфиденциальности и специфики информации.    * Служебная (официальная) информация: Информация, предназначенная для использования в служебных целях органов государственного управления и управления других организаций.    * Конфиденциальная информация: Информация, содержание которой не должно быть раскрыто третьим лицам без согласия её владельца, если иное не предусмотрено законодательством или договором.    * Специальная (персональная) информация: Информация, относящаяся к персональным данным граждан, которая должна быть защищена в соответствии с законодательством о персональных данных. 3. **Секретная информация:** Информация, составляющая государственную тайну или коммерческую тайну, доступ к которой ограничен в соответствии с законодательством Республики Беларусь. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 6 |
| 1. Аудит событий безопасности в ОС Windows, Управление. Основные группы событий.  Управление аудитом событий безопасности в ОС Windows:  1. **Включение аудита:**    * Вход в административные инструменты Windows.    * Переход к "Локальная политика безопасности" или "Групповая политика".    * Настройка параметров аудита в разделе "Правила аудита" (Audit Policy). 2. **Определение параметров:**    * Определение, какие события будут аудитироваться (успешные, неудачные или оба типа).    * Выбор категорий событий для аудита (вход в систему, изменение файлов, административные операции и т. д.). 3. **Хранение аудиторских данных:**    * Установка настроек хранения аудиторских журналов, включая максимальный размер и способы перезаписи данных.  Основные группы событий аудита безопасности в ОС Windows:  1. **Аутентификация (Logon/Logoff):**    * События, связанные с процессом входа и выхода пользователей в систему.    * Примеры: успешный вход в систему, неудачные попытки входа. 2. **Успешные входы (Successful Logons):**    * События, когда пользователь успешно аутентифицирован в системе.    * Пример: успешное вход в систему с использованием имени пользователя и пароля. 3. **Неудачные входы (Failed Logons):**    * События, когда произошла неудачная попытка аутентификации пользователя.    * Пример: неудачная попытка входа в систему с неверным паролем. 4. **Использование объектов (Object Access):**    * События, связанные с доступом к объектам (файлы, папки, реестр и т. д.) в системе.    * Пример: доступ к файлу или папке, изменение прав доступа. 5. **Привилегированные операции (Privilege Use):**    * События, связанные с использованием привилегированных операций в системе.    * Пример: использование привилегий администратора или изменение системных настроек. 6. **Административные действия (Administrative Actions):**    * События, связанные с выполнением административных действий в системе.    * Пример: установка программного обеспечения, изменение настроек безопасности. 7. **Системные события (System Events):**    * События, связанные с работой системы и её компонентов.    * Примеры: перезагрузка системы, сбой службы. 8. Классификация служебной информации ограниченного распространения.   Служебная информация ограниченного распространения представляет собой данные, которые не являются общедоступными и требуют особого режима доступа. Классификация такой информации осуществляется в соответствии с уровнем их конфиденциальности и важности для функционирования организации. В зависимости от специфики деятельности и требований безопасности, служебная информация может быть подразделена на следующие категории:   1. **Внутренняя информация:**    * Данные, предназначенные для использования внутри организации и не предназначенные для общего доступа.    * Включает в себя стратегические планы, финансовые отчеты, договора, внутренние процедуры и политики. 2. **Персональная информация:**    * Данные, относящиеся к персоналу организации или её клиентам, которые требуют особого внимания к конфиденциальности.    * Включает в себя персональные данные сотрудников (ФИО, адреса, телефоны), данные о зарплате, медицинские записи, информацию о клиентах (личные данные, финансовая информация). 3. **Коммерческая информация:**    * Данные, относящиеся к бизнес-процессам, продуктам и услугам компании, которые могут быть ценными для конкурентов.    * Включает в себя конфиденциальные данные о продуктах, технологиях, маркетинговых стратегиях, клиентской базе, ценовой политике. 4. **Интеллектуальная собственность:**    * Данные, представляющие ценность в виде авторских прав, патентов, торговых марок, коммерческих секретов.    * Включает в себя программное обеспечение, дизайн продуктов, технологии, инновации, планы развития. 5. **Секретная информация:**    * Данные, составляющие государственную или коммерческую тайну, требующие особой защиты и ограниченного доступа.    * Включает в себя государственные секреты, коммерческие секреты, конфиденциальные документы. 6. **Защищенная медицинская информация:**    * Данные, содержащие медицинскую и здравоохранительную информацию, подлежащие особой защите согласно законодательству о медицинской конфиденциальности.    * Включает в себя медицинские записи, диагнозы, истории болезней, информацию о здоровье. |
| Экзаменационный билет № 7 |
| 1. Межсетевой экран ОС Windows. Уровни правил фильтрации.   Межсетевой экран (Firewall) в операционной системе Windows представляет собой средство защиты сетевого соединения, которое позволяет контролировать трафик, проходящий через компьютер, и обеспечивает безопасность сети. Он работает на уровне сетевого стека и фильтрует пакеты данных на основе определенных правил. Уровни правил фильтрации в межсетевом экране Windows:  1. **Профили сети:**    * **Общедоступная сеть:** Профиль, применяемый к сетевому подключению, если он определен как "Общественная".    * **Частная сеть:** Профиль, применяемый к сетевому подключению, если он определен как "Частная".    * **Домашняя сеть:** Профиль, применяемый к сетевому подключению, если он определен как "Домашняя". 2. **Входящие правила (Inbound Rules):**    * Контролируют входящий сетевой трафик, направленный на компьютер.    * Определяют, какие типы трафика разрешены или запрещены для получения компьютером. 3. **Исходящие правила (Outbound Rules):**    * Контролируют исходящий сетевой трафик, исходящий из компьютера.    * Определяют, какие типы трафика разрешены или запрещены для отправки компьютером. 4. **Системные правила (System Rules):**    * Автоматически создаваемые правила, управляемые операционной системой.    * Обычно используются для обеспечения работы встроенных сервисов и функциональности ОС. 5. **Пользовательские правила (Custom Rules):**    * Созданные и настроенные пользователем правила фильтрации трафика.    * Позволяют определить конкретные требования безопасности и ограничения доступа к сетевым ресурсам.  Принцип работы:  * Каждое правило содержит определенные условия (например, порт, IP-адрес, протокол) и действия (разрешить, запретить). * Пакеты данных сравниваются с этими правилами, и в зависимости от совпадений принимается решение о передаче или блокировке трафика. * Приоритет правил определяет последовательность их применения: сначала применяются более специфичные правила, затем более общие.  1. Виды информационных ресурсов. Правовой режим информационных ресурсов.   **Виды информационных ресурсов:**   1. **Данные:**    * Основная единица информации, представленная в цифровой форме.    * Включает в себя текстовые документы, изображения, аудио- и видеофайлы, таблицы, базы данных и т. д. 2. **Программное обеспечение:**    * Набор программных инструкций, выполняемых компьютером, для решения определенных задач.    * Включает в себя операционные системы, прикладное программное обеспечение, утилиты и драйверы. 3. **Информационные системы:**    * Комплекс взаимосвязанных компонентов (аппаратное и программное обеспечение, данные, процедуры), предназначенных для сбора, хранения, обработки, анализа и распространения информации. 4. **Сетевые ресурсы:**    * Информационные ресурсы, доступные по сети.    * Включает в себя веб-сайты, базы данных, облачные сервисы, электронные письма, файлы, расположенные на удаленных серверах, и т. д. 5. **Электронные документы:**    * Документы, созданные и хранимые в электронном виде.    * Включает в себя текстовые файлы, электронные таблицы, презентации, электронные книги и т. д. 6. **Автоматизированные системы управления информацией:**    * Системы, предназначенные для автоматизации процессов управления информацией в организации.    * Включает в себя системы управления документооборотом, управления контентом, управления проектами и др.   **Правовой режим информационных ресурсов:**   1. **Авторское право:**    * Законы, регулирующие права авторов на создание и использование информационных ресурсов.    * Включает в себя защиту авторских прав на программное обеспечение, тексты, изображения и другие типы контента. 2. **Законодательство о защите персональных данных:**    * Нормативные акты, определяющие права и обязанности субъектов персональных данных и требования к их обработке и защите.    * Включает в себя законы и нормативные акты о конфиденциальности и защите персональных данных граждан. 3. **Законодательство о информационной безопасности:**    * Нормативные акты, регулирующие требования к защите информационных ресурсов от угроз безопасности.    * Включает в себя законы о защите от кибератак, противодействие киберпреступности и т. д. 4. **Законодательство о коммерческой тайне:**    * Нормативные акты, определяющие правовой статус коммерческой тайны и меры по её защите.    * Включает в себя законы о недопущении несанкционированного доступа к коммерческой информации и предотвращении утечек конфиденциальной информации. 5. **Законодательство о защите информации:**    * Нормативные акты, устанавливающие требования к защите информационных ресурсов в целом.    * Включает в себя законы о безопасности информации, криптографической защите данных, защите от утечек и т. д. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 8 |
| 1. Требования законодательства Республике Беларусь в сфере информационной безопасности.   Законодательство Республики Беларусь в сфере информационной безопасности регулирует различные аспекты защиты информации и обеспечения безопасности информационных технологий. Вот некоторые из основных требований, установленных законодательством Беларуси:   1. **Закон Республики Беларусь "О защите информации"**:    * Определяет основные положения по защите информации во всех её формах.    * Устанавливает правовые основы защиты информации в информационных системах и сетях, а также права и обязанности субъектов информационных отношений. 2. **Закон Республики Беларусь "О персональных данных"**:    * Регулирует обработку персональных данных и устанавливает права граждан на защиту своей конфиденциальной информации.    * Определяет требования к сбору, хранению, использованию и распространению персональных данных, включая меры по их защите. 3. **Закон Республики Беларусь "О защите от компьютерных программ и баз данных"**:    * Регламентирует вопросы защиты авторских прав на компьютерные программы и базы данных.    * Устанавливает ответственность за нарушение авторских прав на программное обеспечение и базы данных. 4. **Постановление Президиума Верховного Совета Республики Беларусь "О мерах по защите информации в информационных системах государственного управления"**:    * Определяет основные меры по защите информации в информационных системах государственного управления.    * Устанавливает требования к организации информационной безопасности в государственных органах. 5. **Национальная стратегия информационной безопасности Республики Беларусь**:    * Устанавливает стратегические цели и приоритеты в области информационной безопасности на государственном уровне.    * Определяет меры по защите информации и развитию сектора информационной безопасности в стране. 6. Государственная регистрация информационных ресурсов.   В Республике Беларусь государственная регистрация информационных ресурсов регламентируется соответствующим законодательством и нормативными актами. Вот основные моменты этой процедуры:   1. **Законодательство:** Вопросы государственной регистрации информационных ресурсов обычно регулируются законодательством о информации, информатизации и защите информации. 2. **Цель регистрации:** Государственная регистрация информационных ресурсов проводится с целью обеспечения контроля за их содержанием, а также для обеспечения общественной безопасности и защиты интересов государства и общества. 3. **Субъекты регистрации:** Обычно подлежат регистрации информационные ресурсы, которые могут оказывать влияние на общественные отношения, имеют особое значение для государства, а также информационные ресурсы, требующие особого режима доступа или обработки. 4. **Органы регистрации:** Государственная регистрация информационных ресурсов может проводиться различными органами, включая государственные агентства по информации, органы по контролю и надзору в сфере информационной безопасности и другие органы исполнительной власти. 5. **Процедура регистрации:** Процедура регистрации может включать подачу заявки на регистрацию информационного ресурса, предоставление необходимых документов и сведений о ресурсе, а также прохождение проверок и экспертиз. 6. **Результат регистрации:** После успешной регистрации информационный ресурс получает соответствующий регистрационный номер или иной идентификационный признак, который подтверждает его легальность и соответствие требованиям законодательства. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 9 |
| 1. Протокол TLS. Назначение. Основные методы аутентификации сторон.   Протокол TLS (Transport Layer Security) представляет собой криптографический протокол, который обеспечивает безопасную передачу данных по сети, обеспечивая конфиденциальность, целостность и аутентификацию. Вот основные его аспекты:  **Назначение:**   1. **Шифрование данных:** Защищает данные, передаваемые между клиентом и сервером, от прослушивания и подмены. 2. **Аутентификация:** Подтверждает подлинность сервера (и иногда клиента), предотвращая атаки перехвата и фальсификации. 3. **Целостность данных:** Гарантирует, что переданные данные не были изменены в процессе передачи.   **Основные методы аутентификации сторон:**   1. **Серверная аутентификация:** Сервер предоставляет свой сертификат клиенту, который подтверждает подлинность сервера. Этот метод является обязательным во всех сессиях TLS. 2. **Клиентская аутентификация:** Если требуется двусторонняя аутентификация, клиент также предоставляет свой сертификат серверу. Это дополнительная мера безопасности и используется в ситуациях, когда необходимо подтверждение идентичности обеих сторон. 3. **Подтверждение аутентификации через пароль:** Этот метод не является стандартным для TLS, однако может быть реализован через дополнительные механизмы, такие как SRP (Secure Remote Password), который позволяет клиенту аутентифицироваться без передачи пароля по сети. 4. **Методы аутентификации с использованием криптографических токенов:** В некоторых случаях могут использоваться аппаратные или программные криптографические токены для аутентификации клиента или сервера. 5. Цели защиты информации.   Защита информации направлена на обеспечение её конфиденциальности, целостности и доступности. Вот основные цели защиты информации:   1. **Конфиденциальность:** Гарантировать, что информация доступна только тем, кто имеет на то право. Это означает предотвращение несанкционированного доступа к конфиденциальным данным, таким как персональные данные, коммерческая информация, государственные секреты и т. д. 2. **Целостность:** Обеспечить неприкосновенность информации, чтобы она не могла быть изменена, повреждена или подделана несанкционированным образом. Это включает в себя предотвращение вмешательства в данные в процессе их передачи или хранения. 3. **Доступность:** Гарантировать, что информация доступна в нужное время и в нужном месте для авторизованных пользователей. Это означает предотвращение отказов в обслуживании, атак на доступность (например, DDoS-атаки) и других угроз, которые могут сделать информацию недоступной. 4. **Аутентификация:** Подтверждение подлинности участников взаимодействия с информацией, таких как пользователи, устройства или программные компоненты. Это позволяет предотвратить несанкционированный доступ к информации и обеспечить её безопасность. 5. **Авторизация:** Управление доступом к информации на основе ролей, полномочий и правил безопасности. Это позволяет ограничивать доступ к чувствительной информации только авторизованным пользователям или группам пользователей. 6. **Невозможность отказа:** Обеспечение невозможности отрицания своих действий или обязательств по отношению к информации. Это важно для обеспечения надежности и доверия в информационных системах и процессах. 7. **Аудит и мониторинг:** Отслеживание действий и событий в информационной системе с целью обнаружения и реагирования на угрозы безопасности, а также обеспечения соответствия политикам безопасности и требованиям законодательства. |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 10 |
| 1. Назначение компонент ОС Андроид: Виртуальная машина Dalvik, Ядро Linux, встроенные библиотеки (Native Libraries).   Компоненты операционной системы Android играют ключевую роль в обеспечении её функциональности и производительности. Вот краткое описание назначения каждого из них:   1. **Виртуальная машина Dalvik (Dalvik Virtual Machine, DVM):**    * *Назначение:* Dalvik VM - это специально разработанная виртуальная машина для выполнения приложений на платформе Android. Она является основным компонентом, который исполняет скомпилированный в байт-код приложений Android (.dex файлы). Одной из особенностей DVM является оптимизация для ограниченных ресурсов мобильных устройств, что помогает повысить производительность приложений. 2. **Ядро Linux:**    * *Назначение:* Ядро Linux является основой операционной системы Android. Оно предоставляет базовые функциональные возможности, такие как управление памятью, управление процессами, файловая система и управление устройствами. Android использует ядро Linux для обеспечения надежной и безопасной работы приложений, а также взаимодействия с аппаратным обеспечением устройства. 3. **Встроенные библиотеки (Native Libraries):**    * *Назначение:* Встроенные библиотеки представляют собой набор компонентов, написанных на языках программирования C и C++, которые обеспечивают доступ к различным системным функциям и ресурсам устройства. Эти библиотеки используются приложениями Android для выполнения задач, таких как взаимодействие с аппаратным обеспечением, обработка графики, работа с сетью и другие операции, требующие быстрого доступа к системным ресурсам. 4. Основные требования по защите информации.   Основные требования по защите информации включают в себя:   1. **Конфиденциальность:**    * Обеспечение доступа к информации только авторизованным пользователям или системам.    * Защита от несанкционированного доступа, прослушивания или просмотра информации. 2. **Целостность:**    * Гарантирование неприкосновенности информации от несанкционированных изменений.    * Предотвращение возможности подмены или повреждения данных в процессе их передачи или хранения. 3. **Доступность:**    * Обеспечение доступности информации в нужное время и место для авторизованных пользователей.    * Предотвращение отказов в обслуживании, атак на доступность и других угроз, которые могут сделать информацию недоступной. 4. **Аутентификация:**    * Подтверждение подлинности участников взаимодействия с информацией (пользователей, систем или устройств).    * Предотвращение несанкционированного доступа путем проверки идентификационных данных. 5. **Авторизация:**    * Управление доступом к информации на основе ролей, полномочий и правил безопасности.    * Обеспечение возможности предоставления доступа к информации только авторизованным пользователям или группам пользователей. 6. **Невозможность отрицания:**    * Обеспечение невозможности отказа в своих действиях или обязательствах по отношению к информации.    * Предотвращение возможности отрицания авторства, отправки сообщения или выполнения действий. 7. **Аудит и мониторинг:**    * Отслеживание действий и событий в информационной системе с целью обнаружения и реагирования на угрозы безопасности.    * Обеспечение соответствия политикам безопасности и требованиям законодательства путем регулярного аудита и мониторинга системы. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 11 |
| 1. Система разрешений для приложений в ОС Android.   Система разрешений для приложений в операционной системе Android предоставляет пользователю контроль над доступом приложений к различным ресурсам и функциям устройства. Вот основные аспекты этой системы:   1. **Разделение на уровни разрешений:**    * Разрешения в Android разделены на различные уровни, такие как разрешения для доступа к контактам, камере, местоположению, хранилищу и другим ресурсам устройства. 2. **Запрос разрешений во время установки:**    * При установке приложения пользователь уведомляется о необходимости доступа к определенным ресурсам.    * Пользователю предоставляется возможность разрешить или отклонить доступ приложения к этим ресурсам. 3. **Динамическое запрос разрешений (с Android 6.0 Marshmallow):**    * С Android 6.0 и более поздних версий разрешения могут запрашиваться динамически во время выполнения приложения.    * Это позволяет пользователям предоставлять или отклонять доступ к ресурсам приложения по мере необходимости. 4. **Система контроля доступа (Permission Control System):**    * Android предоставляет систему контроля доступа, которая отслеживает и управляет разрешениями приложений на устройстве.    * Пользователи могут просматривать и изменять разрешения для установленных приложений в настройках устройства. 5. **Обязательные разрешения и разрешения для опасных операций:**    * Некоторые разрешения считаются обязательными для выполнения определенных операций, таких как отправка SMS или запрос местоположения.    * Разрешения для выполнения таких операций считаются опасными и могут потребовать дополнительного согласия пользователя. 6. **Расширенные разрешения (Runtime Permissions):**    * Некоторые разрешения требуют специальной обработки и запроса на время выполнения, например, доступ к камере или микрофону. 7. Классификация мер по защите информации.   Меры по защите информации могут быть классифицированы по различным критериям. Вот несколько основных классификаций:   1. **По типу угроз:**    * **Технические меры:** Направлены на защиту информации от компьютерных атак, вирусов, хакерских атак и других технических угроз.    * **Организационные меры:** Охватывают политики, процедуры и практики управления информационной безопасностью, такие как обучение персонала, управление доступом и аудит безопасности.    * **Физические меры:** Включают в себя защиту физического доступа к информации путем использования замков, систем контроля доступа и видеонаблюдения. 2. **По области применения:**    * **Превентивные меры:** Направлены на предотвращение возникновения угроз и инцидентов безопасности. Например, установка антивирусного ПО или настройка брандмауэров.    * **Детективные меры:** Направлены на обнаружение угроз и инцидентов безопасности. Например, системы мониторинга и аудита безопасности.    * **Корректирующие меры:** Направлены на восстановление системы или данных после инцидента безопасности. Например, создание резервных копий данных и восстановление после атаки. 3. **По уровню защиты:**    * **Физические меры:** Обеспечивают защиту физического доступа к системам и оборудованию.    * **Логические меры:** Обеспечивают защиту данных и информационных систем с использованием криптографии, аутентификации и авторизации.    * **Административные меры:** Обеспечивают управление и контроль над процессами безопасности, такие как политики безопасности, обучение персонала и управление рисками. 4. **По области применения:**    * **Сетевая безопасность:** Включает меры защиты сетей, маршрутизаторов, брандмауэров и других сетевых устройств.    * **Компьютерная безопасность:** Направлена на защиту компьютеров, серверов и операционных систем от вирусов, хакерских атак и других угроз.    * **Информационная безопасность:** Обеспечивает защиту информации в целом, включая её сбор, обработку, хранение и передачу. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 12 |
| 1. Разграничение доступа к объектам ОС Windows.   Разграничение доступа к объектам в операционной системе Windows играет важную роль в обеспечении безопасности информации и ресурсов системы. Вот основные аспекты разграничения доступа:   1. **Пользователи и группы:**    * Windows использует систему пользователей и групп для управления доступом к объектам. Пользователи могут быть назначены в различные группы, что позволяет управлять правами доступа на групповом уровне. 2. **ACL (Access Control Lists):**    * Каждый объект в Windows (файл, папка, реестр и т. д.) имеет свой список контроля доступа (ACL), который определяет, кто имеет доступ к этому объекту и какие разрешения у них есть.    * В ACL указываются пользователи или группы, а также их разрешения (чтение, запись, выполнение и т. д.). 3. **Ролевые службы (Role-Based Services):**    * Windows Server поддерживает концепцию ролевых служб, которая позволяет назначать роли пользователям и группам в зависимости от их функциональных обязанностей или требований безопасности.    * Ролевые службы обеспечивают более гибкое и эффективное управление доступом к объектам. 4. **Управление политиками безопасности (Security Policies Management):**    * Windows предоставляет средства управления политиками безопасности, которые позволяют администраторам определять правила доступа к объектам на уровне системы.    * С помощью политик безопасности можно установить требуемые стандарты безопасности, ограничения доступа и многое другое. 5. **Аудит доступа (Access Auditing):**    * Windows позволяет вести журнал аудита доступа, в котором записываются события, связанные с доступом к объектам.    * Аудит доступа позволяет отслеживать попытки несанкционированного доступа и проводить анализ безопасности системы. 6. Права и обязанности субъектов информационных отношений по защите информации.   Субъекты информационных отношений, включая как физических лиц, так и юридических лиц, обладают определенными правами и обязанностями по защите информации. Вот основные из них:  **Права субъектов:**   1. **Право на конфиденциальность:** Субъекты имеют право на защиту своей конфиденциальной информации от несанкционированного доступа и раскрытия. 2. **Право на целостность данных:** Субъекты имеют право на то, чтобы их данные не подвергались изменениям или повреждениям без их согласия. 3. **Право на доступность:** Субъекты имеют право на доступ к информации, необходимой для выполнения их задач и функций. 4. **Право на информационную безопасность:** Субъекты имеют право на защиту своей информации от угроз безопасности, таких как вирусы, хакерские атаки и другие. 5. **Право на прозрачность:** Субъекты имеют право на получение информации о том, как их данные используются и обрабатываются.   **Обязанности субъектов:**   1. **Соблюдение политик и правил безопасности:** Субъекты обязаны соблюдать политики и правила безопасности, установленные организацией или законодательством. 2. **Соблюдение конфиденциальности:** Субъекты обязаны сохранять конфиденциальность информации, к которой у них есть доступ, и не разглашать её без необходимости. 3. **Использование безопасных практик:** Субъекты обязаны использовать безопасные практики при работе с информацией, такие как создание надежных паролей и обновление программного обеспечения. 4. **Сообщение об угрозах безопасности:** Субъекты обязаны сообщать об ожидаемых или обнаруженных угрозах безопасности информации организации или компетентным органам. 5. **Соблюдение законодательства:** Субъекты обязаны соблюдать требования законодательства в области защиты информации, включая правила обработки и хранения данных. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 13 |
| 1. Изоляция прикладных процессов в ОС Windows.   Изоляция прикладных процессов в операционной системе Windows играет ключевую роль в обеспечении безопасности и стабильности системы. Вот основные методы и механизмы, используемые для этой цели:   1. **Пользовательские учетные записи (User Accounts):**    * Windows использует механизм пользовательских учетных записей для разделения приложений и процессов между разными пользователями.    * Каждый пользователь имеет свою собственную среду выполнения, включая файловую систему и реестр, что обеспечивает изоляцию данных и настроек между пользователями. 2. **Виртуализация и контейнеризация:**    * С помощью технологий виртуализации, таких как Hyper-V и контейнеризации, таких как Docker, можно создавать изолированные среды выполнения для приложений и сервисов.    * Эти изолированные контейнеры обеспечивают высокий уровень безопасности и позволяют изолировать процессы друг от друга. 3. **AppContainer и Windows Sandbox:**    * Windows включает в себя технологию AppContainer, которая обеспечивает изоляцию приложений с помощью ограничений доступа к ресурсам системы.    * Windows Sandbox предоставляет изолированную среду для запуска ненадежных приложений, которые могут быть потенциально вредоносными. 4. **UAC (User Account Control):**    * Механизм контроля учетных записей пользователя (UAC) в Windows обеспечивает повышение привилегий только для действий, требующих административных прав.    * Это помогает предотвратить несанкционированные изменения в системных файлах и настройках. 5. **Изолированные процессы:**    * Windows может запускать приложения в изолированных процессах, что помогает предотвратить повреждение системы или других приложений в случае сбоя или атаки. 6. Отнесение к общедоступной информации.   Общедоступная информация - это информация, которая доступна для всеобщего использования без каких-либо ограничений или специального разрешения. Отнесение к общедоступной информации означает, что данная информация может быть свободно доступна всем пользователям без ограничений или ограничена лишь минимальными условиями. Вот некоторые примеры отнесения к общедоступной информации:   1. **Публичные интернет-ресурсы:** Информация, доступная через общедоступные веб-сайты или онлайн-платформы без необходимости аутентификации или авторизации. 2. **Публичные библиотеки и архивы:** Книги, журналы, статьи, аудио- и видеозаписи, которые доступны для чтения и прослушивания в общедоступных библиотеках и архивах. 3. **Публичные базы данных:** Данные, предоставленные организациями или государственными учреждениями в открытых базах данных, которые могут быть свободно загружены и использованы. 4. **Публичные исследования и отчеты:** Результаты исследований, отчеты, статистика и другие документы, опубликованные с целью распространения информации в широком доступе. 5. **Открытые правительственные данные:** Данные, предоставленные правительственными органами для общественного использования, такие как законы, бюджеты, географические данные и т. д. 6. **Общественные записи:** Информация, доступная в общественных записях, таких как реестры недвижимости, свидетельства о рождении и смерти, судебные документы и т. д. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 14 |
| 1. Назначение и принцип работы сервиса EFS в ОС Windows.   Служба шифрования файлов (EFS) в операционной системе Windows предназначена для защиты конфиденциальных данных путем шифрования файлов и папок на уровне файловой системы. Её принцип работы основан на использовании симметричного шифрования и асимметричного шифрования с открытым ключом. Вот основные задачи и принципы работы EFS:   1. **Назначение:**    * Защита конфиденциальных данных пользователей путем шифрования файлов и папок на уровне файловой системы.    * Обеспечение безопасного доступа к зашифрованным данным только авторизованным пользователям или системам. 2. **Принцип работы:**    * **Симметричное шифрование:** При создании файла или папки с помощью EFS генерируется случайный ключ шифрования, который используется для зашифрования и расшифрования данных. Этот ключ шифруется с помощью открытого ключа пользователя и хранится в зашифрованной форме в атрибутах файла.    * **Асимметричное шифрование с открытым ключом:** Для доступа к зашифрованным данным требуется закрытый ключ пользователя, который используется для расшифрования симметричного ключа шифрования.    * **Прозрачность для пользователя:** Пользователи могут зашифровывать и расшифровывать файлы и папки с помощью обычных операций копирования, перемещения и открытия файлов.    * **Использование сертификатов для доступа:** Для доступа к зашифрованным данным пользователи могут использовать сертификаты, которые обеспечивают аутентификацию и авторизацию. 3. **Дополнительные возможности:**    * EFS позволяет создавать и управлять сертификатами для шифрования и расшифрования данных, а также управлять правами доступа к зашифрованным файлам и папкам.    * EFS также обеспечивает возможность резервного копирования и восстановления ключей шифрования для предотвращения потери доступа к зашифрованным данным в случае утери или повреждения ключей. 4. Распространение и (или) предоставление информации.   Распространение и предоставление информации - это процессы передачи информации от одного источника к другому или предоставления доступа к информации конкретным лицам или организациям. Вот некоторые основные аспекты этих процессов:   1. **Распространение информации:**    * **Цифровое распространение:** Передача информации по сети Интернет, включая электронную почту, веб-сайты, социальные сети, мессенджеры и т. д.    * **Аналоговое распространение:** Распространение информации через традиционные средства, такие как печатные издания, телевидение, радио, брошюры, листовки и т. д.    * **Персональное распространение:** Передача информации от человека к человеку, например, устное общение, презентации, семинары, конференции и т. д. 2. **Предоставление информации:**    * **Активное предоставление:** Предоставление информации по запросу конкретных лиц или организаций, например, в ответ на запросы клиентов, запросы информации из государственных органов, обращения от партнеров и т. д.    * **Пассивное предоставление:** Предоставление информации без предварительного запроса, например, публикация информации на веб-сайтах, в социальных сетях, размещение информационных брошюр и листовок в офисах или на площадках, и т. д. 3. **Виды информации, подлежащей распространению и предоставлению:**    * **Открытая информация:** Информация, доступная для всеобщего использования без ограничений.    * **Ограниченная информация:** Информация, доступ к которой ограничен определенным кругом лиц или организаций из-за конфиденциальности, коммерческих секретов, правовых ограничений или других причин.    * **Чувствительная информация:** Информация, требующая особого внимания и мер безопасности при её распространении и предоставлении, такая как медицинские данные, банковская информация, персональные данные и т. д. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 15 |
| 1. Обзор используемых мобильных операционных систем. Основные компоненты.   Обзор используемых мобильных операционных систем (ОС) может включать в себя такие системы, как Android, iOS и HarmonyOS (также известная как HongMeng в Китае). Вот краткий обзор основных компонентов каждой из них:   1. **Android:**    * **Ядро Linux:** Основа операционной системы, обеспечивающая работу аппаратных устройств и базовые функции.    * **Android Runtime (ART):** Среда выполнения приложений, в которой выполняются приложения Android. В Android 5.0 и выше используется компиляция Ahead-of-Time (AOT).    * **Android Framework:** Набор API и инструментов разработки, предоставляющий разработчикам доступ к различным функциям устройства, таким как управление экраном, доступ к камере, сетевым функциям и т. д.    * **User Interface (UI):** Интерфейс пользователя, включающий в себя домашний экран, меню приложений, уведомления и другие элементы управления.    * **Google Play Services:** Набор служб и API, предоставляемых Google, таких как карты, аутентификация, облачные услуги и другие, упрощающие разработку приложений и предоставление пользовательских сервисов. 2. **iOS:**    * **Darwin Kernel:** Ядро операционной системы, основанное на BSD и Mach, обеспечивает основные функции устройства.    * **UIKit:** Фреймворк, предоставляющий инструменты для создания пользовательского интерфейса и управления событиями взаимодействия с пользователем.    * **Core Services:** Набор служб и библиотек, включающих Foundation, CoreData, CoreGraphics и CoreAnimation, обеспечивающих базовые функции и возможности работы с данными.    * **App Framework:** Фреймворк, обеспечивающий жизненный цикл приложений, управление памятью, мультимедийные возможности и другие базовые функции.    * **App Store:** Официальный магазин приложений для iOS, предоставляющий доступ к миллионам приложений и игр для пользователей. 3. **HarmonyOS (HongMeng):**    * **Microkernel Architecture:** Микроядерная архитектура, обеспечивающая высокую эффективность и гибкость, а также возможность работы на различных устройствах.    * **Distributed Capabilities:** Возможность распределенных вычислений и управления устройствами, позволяющая создавать разнообразные сценарии взаимодействия и совместного использования ресурсов.    * **DevEco Studio:** Интегрированная среда разработки, предоставляющая инструменты для создания приложений и сервисов для HarmonyOS.    * **Huawei AppGallery:** Официальный магазин приложений, предлагающий пользователю доступ к разнообразным приложениям и сервисам для устройств на HarmonyOS. 4. Организация защиты информации.   Организация защиты информации - это комплексный процесс, включающий в себя различные меры, политики, процедуры и технологии, направленные на обеспечение конфиденциальности, целостности и доступности информации. Вот основные аспекты организации защиты информации:   1. **Оценка угроз и рисков:**    * Проведение анализа угроз и оценки рисков для выявления потенциальных угроз безопасности информации и определения уровня их влияния на организацию. 2. **Разработка политик и стандартов:**    * Создание политик безопасности информации, которые определяют основные принципы, правила и процедуры обеспечения безопасности, а также стандартов, которые конкретизируют требования к защите информации. 3. **Развертывание технических средств защиты:**    * Реализация технических средств защиты информации, таких как антивирусное ПО, межсетевые экраны, средства шифрования данных, системы обнаружения вторжений и т. д. 4. **Обеспечение физической безопасности:**    * Принятие мер по обеспечению безопасности физических ресурсов, таких как серверные помещения, центры обработки данных, компьютеры и другие устройства. 5. **Обучение и осведомленность сотрудников:**    * Проведение обучения сотрудников по вопросам информационной безопасности, а также повышение их осведомленности о возможных угрозах и мерах защиты. 6. **Управление доступом:**    * Установление политики управления доступом к информации, включая разграничение прав доступа пользователей, многофакторную аутентификацию, управление привилегиями и т. д. 7. **Мониторинг и аудит безопасности:**    * Проведение постоянного мониторинга системы защиты информации, а также аудита безопасности для выявления возможных нарушений и незаконных действий. 8. **Инцидентный реагирование и восстановление:**    * Разработка планов реагирования на инциденты безопасности и восстановления после них, включая процедуры обнаружения, реагирования, документирования и анализа инцидентов. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 16 |
| 1. Угрозы информационной безопасности мобильных ОС. Классификация.   Угрозы информационной безопасности мобильных операционных систем (ОС) включают разнообразные атаки и уязвимости, которые могут привести к утечке конфиденциальной информации, нарушению целостности данных и ограничению доступности сервисов. Вот классификация основных угроз информационной безопасности мобильных ОС:   1. **Вредоносные программы (Malware):**    * **Вирусы:** Злонамеренные программы, которые могут самостоятельно распространяться и инфицировать другие приложения или файлы на устройстве.    * **Шпионское ПО:** Программы, которые собирают конфиденциальную информацию о пользователе без его согласия, такую как личные данные, пароли, банковские данные и т. д.    * **Рекламное ПО (Adware):** Программы, которые показывают назойливую рекламу и могут собирать персональную информацию для таргетирования рекламы.    * **Руткиты:** Скрытые программы, которые позволяют злоумышленникам получать полный контроль над устройством и обходить системные меры безопасности. 2. **Фишинг и Социальная инженерия:**    * Атаки, которые используют манипуляции и обман для обмана пользователей и получения доступа к их учетным данным, паролям и другой конфиденциальной информации. 3. **Уязвимости и эксплойты:**    * **Уязвимости в приложениях:** Недостатки в программном обеспечении, которые могут быть использованы злоумышленниками для выполнения вредоносного кода или получения несанкционированного доступа к устройству.    * **Уязвимости в операционной системе:** Недостатки в самой мобильной ОС, которые могут быть использованы для обхода защитных механизмов и получения контроля над устройством.    * **Эксплойты мобильных браузеров:** Атаки, которые используют уязвимости в мобильных браузерах для внедрения вредоносного кода или перенаправления на фальшивые веб-сайты. 4. **Утеря или кража устройства:**    * Потеря или кража мобильного устройства, что может привести к доступу к конфиденциальной информации, если данные на устройстве не зашифрованы или не защищены. 5. **Сетевые атаки:**    * **Ман-в-середине (Man-in-the-Middle, MITM):** Атаки, при которых злоумышленник перехватывает и манипулирует сетевым трафиком между устройством и интернетом.    * **Атаки отказа в обслуживании (Denial-of-Service, DoS):** Попытки злоумышленников перегрузить сетевые ресурсы или сервисы, чтобы привести к отказу в доступе к ним. 6. **Неавторизованный доступ к данным:**    * Нарушение прав доступа к конфиденциальным данным пользователей или корпоративным ресурсам, которое может произойти из-за слабых паролей, недостаточной аутентификации или утечки учетных данных. 7. Права и обязанности субъектов информационных отношений по защите информации.   Права и обязанности субъектов информационных отношений по защите информации определяются как законодательством, так и внутренними политиками и процедурами организаций. Вот основные аспекты прав и обязанностей:   1. **Права субъектов:**    * **Право на конфиденциальность:** Пользователи имеют право на защиту конфиденциальности своих персональных данных и другой чувствительной информации.    * **Право на безопасность:** Пользователи имеют право на защищенное использование информационных систем и сервисов без риска утечки данных или других угроз безопасности.    * **Право на доступность информации:** Пользователи имеют право на доступ к необходимой информации в соответствии с их задачами и обязанностями. 2. **Обязанности субъектов:**    * **Соблюдение политик безопасности:** Пользователи обязаны соблюдать установленные организацией или государственными структурами политики и стандарты безопасности информации.    * **Защита конфиденциальности данных:** Пользователи обязаны предпринимать меры по защите конфиденциальности данных, с которыми они работают, включая установку сильных паролей, шифрование данных и другие меры безопасности.    * **Информирование о нарушениях:** Пользователи обязаны немедленно информировать администраторов или ответственных лиц о любых нарушениях безопасности или инцидентах, которые могли привести к утечке информации или другим угрозам.    * **Обучение и осведомленность:** Пользователи обязаны проходить обучение и повышать свою осведомленность о мерах безопасности информации, а также о новых угрозах и методах защиты. 3. **Ответственность за нарушения:**    * Пользователи могут нести ответственность за нарушения политик безопасности или неправильное использование информационных ресурсов, что может привести к утрате или компрометации конфиденциальной информации.    * Организации могут принимать различные меры дисциплинарного, административного или юридического характера в отношении субъектов, нарушающих правила и политики безопасности. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 17 |
| 1. Системы лицензирования Android-приложений.   Системы лицензирования для Android-приложений представляют собой механизмы, которые разработчики могут использовать для защиты своих приложений от нелегального использования и распространения. Вот несколько основных систем лицензирования для Android-приложений:   1. **Google Play Licensing:**    * Это официальная система лицензирования, предоставляемая Google для разработчиков приложений, размещаемых в Google Play Store.    * Google Play Licensing позволяет разработчикам связывать свои приложения с Google Play, что обеспечивает контроль над лицензиями и управление доступом к приложениям через Google Play. 2. **Пользовательские ключи и лицензии:**    * Разработчики могут создавать собственные системы лицензирования на основе пользовательских ключей и лицензий.    * Это может включать в себя генерацию уникальных ключей лицензии для каждого пользователя и проверку этих ключей на стороне сервера при запуске приложения. 3. **Online Activation:**    * Этот метод включает в себя требование активации приложения через интернет перед его использованием.    * Приложение связывается с сервером разработчика для проверки действительности лицензии перед тем, как пользователь сможет начать его использование. 4. **Hardware-based Licensing:**    * Некоторые разработчики могут использовать аппаратные функции устройства для защиты своих приложений.    * Это может включать в себя использование уникальных идентификаторов устройства или других аппаратных компонентов для связывания с лицензией приложения. 5. **Облачные сервисы:**    * Разработчики могут использовать облачные сервисы для управления лицензиями и доступом к своим приложениям.    * Это позволяет централизованно управлять лицензиями, обновлениями и мониторингом использования приложений. 6. Защита персональных данных.   Защита персональных данных - это процесс обеспечения конфиденциальности, целостности и доступности информации о личности, которая может быть использована для идентификации конкретного человека. Вот несколько основных аспектов защиты персональных данных:   1. **Соблюдение законодательства:**    * Организации и предприятия должны соблюдать соответствующие законы и нормативные акты, регулирующие обработку и защиту персональных данных, такие как GDPR в Европейском Союзе или CCPA в Калифорнии. 2. **Методы шифрования:**    * Использование шифрования данных для защиты информации в покое (at rest) и в движении (in transit), что предотвращает несанкционированный доступ к персональным данным в случае утечки или проникновения. 3. **Управление доступом:**    * Ограничение доступа к персональным данным только соответствующим и авторизованным сотрудникам и системам.    * Реализация принципа "минимальных привилегий", когда доступ к данным предоставляется только в том объеме, который необходим для выполнения конкретных задач. 4. **Обучение персонала:**    * Проведение обучения и повышения осведомленности сотрудников о правилах и процедурах защиты персональных данных, а также о методах и средствах предотвращения инцидентов безопасности. 5. **Аудит и мониторинг:**    * Регулярное проведение аудитов безопасности и мониторинга систем для выявления и предотвращения утечек или несанкционированного доступа к персональным данным. 6. **Обеспечение физической безопасности:**    * Защита физических местоположений, где хранятся или обрабатываются персональные данные, от несанкционированного доступа или кражи. 7. **Соблюдение принципов прозрачности и информирования:**    * Предоставление пользователю прозрачной информации о целях и методах обработки его персональных данных, а также о правах, которые он имеет в отношении своих данных. 8. **Быстрое реагирование на инциденты:**    * Разработка планов реагирования на инциденты и реализация мер по быстрому обнаружению, реагированию и устранению нарушений безопасности данных. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 18 |
| 1. Механизм авторизованного доступа к объекту в ОС Windows.   Механизм авторизованного доступа к объекту в операционной системе Windows основан на системе управления доступом (Access Control). Вот основные компоненты и принципы этого механизма:   1. **Субъекты и объекты:**    * **Субъекты:** Это пользователи, группы пользователей или процессы, которые пытаются получить доступ к объектам.    * **Объекты:** Это файлы, папки, ресурсы сети, реестр Windows и другие элементы, к которым предпринимается попытка доступа. 2. **Дискреционный контроль доступа (Discretionary Access Control, DAC):**    * DAC определяет права доступа к объектам, которые контролируются владельцами объектов. Каждый объект имеет список контроля доступа (Access Control List, ACL), который содержит записи о правах доступа для конкретных пользователей или групп.    * Владелец объекта может устанавливать права доступа (чтение, запись, выполнение и т. д.) для других пользователей или групп, а также изменять эти права по своему усмотрению. 3. **Объекты безопасности (Security Objects):**    * В Windows каждый объект, такой как файл или папка, является объектом безопасности, который имеет свои атрибуты безопасности и список контроля доступа.    * Объекты безопасности имеют уникальные идентификаторы безопасности (SID), которые используются для идентификации субъектов, имеющих доступ к объекту. 4. **Привилегии (Privileges):**    * Привилегии определяют действия, которые субъекты могут выполнять на объектах в операционной системе Windows.    * Привилегии могут быть назначены пользователям или группам и позволяют выполнение привилегированных операций, таких как управление службами, изменение настроек безопасности и т. д. 5. **Принцип наименьших привилегий (Principle of Least Privilege, POLP):**    * POLP предполагает, что субъекты должны иметь только те привилегии, которые необходимы для выполнения своих задач, чтобы минимизировать риски безопасности в случае компрометации. 6. **Проверка подлинности (Authentication) и авторизация (Authorization):**    * Проверка подлинности определяет идентичность субъекта, пытающегося получить доступ к объекту.    * Авторизация определяет, имеет ли субъект права доступа к объекту в соответствии с правилами DAC и привилегиями. 7. Правила размещения на рынке или ввода в эксплуатацию средств защиты информации.   Правила размещения на рынке или ввода в эксплуатацию средств защиты информации могут различаться в зависимости от страны и региона, но обычно они включают в себя следующие аспекты:   1. **Сертификация и лицензирование:**    * Производители средств защиты информации могут быть обязаны проходить сертификацию или лицензирование перед тем, как их продукты могут быть размещены на рынке или использоваться в организациях.    * Эти процедуры обычно включают в себя тестирование безопасности продукта и подтверждение его соответствия стандартам и требованиям безопасности. 2. **Соблюдение нормативных актов и стандартов:**    * Производители должны соблюдать нормативные акты и стандарты в области информационной безопасности, установленные соответствующими государственными органами или регуляторами.    * Это может включать в себя соблюдение законодательства о защите персональных данных, стандарты криптографии, требования к защите информации в критической инфраструктуре и другие нормативные акты. 3. **Документация и техническая информация:**    * Производители должны предоставить полную документацию и техническую информацию о своих средствах защиты информации, включая инструкции по установке, настройке и эксплуатации, а также спецификации безопасности. 4. **Обучение и поддержка пользователей:**    * Пользователи средств защиты информации должны быть обучены использованию этих средств и ознакомлены с их основными функциями и возможностями.    * Производители должны предоставить поддержку и техническую помощь пользователям в случае возникновения проблем или вопросов. 5. **Регистрация и отчетность:**    * В некоторых случаях производители или поставщики средств защиты информации могут быть обязаны регистрировать свои продукты у соответствующих органов и предоставлять отчеты о продажах или использовании. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 19 |
| 1. Назначение и принцип работы сервиса Bitlocker в ОС Windows.   BitLocker - это сервис шифрования дисков, предоставляемый операционной системой Windows. Его основное назначение - защита данных на диске путем их шифрования. Вот основные принципы работы и назначение сервиса BitLocker:   1. **Назначение:**    * Защита конфиденциальности данных путем шифрования содержимого дискового раздела.    * Предотвращение несанкционированного доступа к данным на диске, в случае утери или кражи устройства.    * Обеспечение соответствия нормативным требованиям по защите конфиденциальной информации. 2. **Принцип работы:**    * **Шифрование диска:** BitLocker использует симметричное шифрование для защиты данных на диске. По умолчанию используется алгоритм AES (Advanced Encryption Standard) с длиной ключа 128 или 256 бит.    * **Ключи шифрования:** При активации BitLocker генерирует ключ шифрования (объемный ключ), который используется для шифрования содержимого диска. Этот ключ зашифровывается с помощью ключа защиты, который можно сохранить на внешнем носителе, в аккаунте Microsoft или в Active Directory (в зависимости от настроек).    * **Процесс разблокировки:** При включении компьютера или доступе к зашифрованному диску BitLocker требует ввода ключа разблокировки (объемного ключа) или кода PIN (при использовании режима PIN) для разблокировки диска и доступа к данным.    * **Интеграция с TPM:** BitLocker может интегрироваться с Trusted Platform Module (TPM) для обеспечения дополнительной безопасности. TPM используется для хранения ключей шифрования, что делает их недоступными для атак в случае физического доступа к диску.    * **Восстановление:** В случае утери ключа шифрования или забытого пароля доступа, BitLocker предоставляет механизмы восстановления, которые позволяют администраторам восстановить доступ к данным. 3. Подтверждение соответствия требованиям информационной безопасности.   Подтверждение соответствия требованиям информационной безопасности - это процесс проверки и подтверждения того, что системы, процессы и практики информационной безопасности соответствуют установленным стандартам, нормативам и политикам. Вот основные этапы этого процесса:   1. **Определение требований безопасности:** Сначала определяются соответствующие требования безопасности, которые могут включать в себя законодательные акты, регуляторные стандарты, отраслевые рекомендации или внутренние политики и стандарты организации. 2. **Анализ текущего состояния:** Проводится анализ текущего состояния системы информационной безопасности, включая оценку угроз, уязвимостей и защищенности систем и данных. 3. **Разработка плана соответствия:** На основе выявленных требований и анализа текущего состояния разрабатывается план действий по достижению соответствия требованиям безопасности. 4. **Внедрение необходимых мер:** После разработки плана соответствия необходимые меры по улучшению информационной безопасности внедряются и реализуются в организации. 5. **Проверка и аудит:** Проводятся проверки и аудиты системы информационной безопасности для оценки эффективности внедренных мер и определения соответствия установленным требованиям. 6. **Корректировка и улучшение:** На основе результатов проверок и аудитов вносятся корректировки и улучшения в систему информационной безопасности для дальнейшего обеспечения соответствия требованиям. 7. **Документирование:** Все этапы процесса подтверждения соответствия должны быть документированы для последующего отчета о статусе и результате проверки. 8. **Сообщение и управление рисками:** Результаты проверки и аудита, а также любые обнаруженные уязвимости или недостатки, должны быть переданы руководству организации для принятия решений и управления рисками информационной безопасности. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 20 |
| 1. Электронная цифровая подпись программного кода.   Электронная цифровая подпись программного кода - это метод обеспечения целостности и подлинности программного обеспечения путем создания и привязки электронной подписи к исполняемому файлу или исходному коду. Вот основные принципы и функции электронной цифровой подписи программного кода:   1. **Принцип работы:**    * Цифровая подпись создается путем хэширования содержимого исполняемого файла или исходного кода с использованием криптографических алгоритмов.    * Полученный хеш-код шифруется с использованием закрытого ключа подписчика, создавая электронную подпись.    * Электронная подпись встроена в исполняемый файл или прикрепляется к исходному коду. 2. **Цели использования:**    * **Подлинность:** Проверка электронной подписи позволяет убедиться, что программный код действительно создан и подписан определенным лицом или организацией.    * **Целостность:** Электронная подпись также обеспечивает защиту от несанкционированных изменений в программном коде после его подписания.    * **Невозможность отказа:** Электронная цифровая подпись также может служить доказательством того, что конкретное лицо или организация действительно подписала программный код и не может отказаться от этого факта. 3. **Проверка подписи:**    * При проверке подписи используется открытый ключ подписчика для расшифровки электронной подписи и получения хеш-кода.    * Полученный хеш-код сравнивается с хеш-кодом программного кода, сгенерированным на момент проверки. Если они совпадают, подпись считается действительной. 4. **Используемые стандарты:**    * Распространенные стандарты для электронных цифровых подписей программного кода включают в себя Authenticode для исполняемых файлов под Windows и код подписи Java (JAR) для Java-приложений. 5. **Безопасность:**    * Безопасность электронной цифровой подписи зависит от безопасности закрытого ключа подписчика. Потеря или компрометация закрытого ключа может привести к возможности подписи недобросовестными лицами. 6. Механизм защиты драйверов режима ядра в ОС Windows10.   В ОС Windows 10 драйверы режима ядра, также известные как Kernel Mode Drivers, являются важной частью операционной системы, поскольку они имеют прямой доступ к ядру операционной системы и могут выполнять привилегированные операции. Для обеспечения безопасности и стабильности системы Microsoft предусматривает несколько механизмов защиты для драйверов режима ядра в Windows 10:   1. **Цифровые подписи:** Драйверы режима ядра должны быть подписаны цифровым сертификатом, выданным доверенным удостоверяющим центром. Это помогает обнаружить измененные или вредоносные драйверы, поскольку Windows проверяет подлинность подписи при загрузке драйвера. 2. **Аттестация драйверов:** Microsoft разработала программу аттестации драйверов, известную как Windows Hardware Quality Labs (WHQL). Драйверы, прошедшие аттестацию WHQL, считаются более надежными и безопасными для использования в Windows 10. 3. **Code Integrity (Целостность кода):** Эта функция Windows 10 обеспечивает контроль над целостностью исполняемых файлов, включая драйверы режима ядра. Она позволяет операционной системе проверять цифровые подписи и хеш-суммы файлов на соответствие ожидаемым значениям, что помогает обнаруживать и предотвращать загрузку измененных или вредоносных файлов. 4. **Driver Signature Enforcement (Принудительное соблюдение подписи драйверов):** Этот механизм защиты в Windows 10 требует, чтобы все загружаемые драйверы были подписаны цифровым сертификатом. Если драйвер не подписан, система может отказать в его загрузке. 5. **Kernel Patch Protection (Защита ядра от изменений):** Этот механизм, также известный как PatchGuard, предназначен для предотвращения изменения ядра операционной системы и мониторит его на предмет попыток модификации со стороны драйверов или приложений |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 21 |
| 1. Архитектура построения системы мобильной ОС Android.   Архитектура мобильной операционной системы Android построена на основе нескольких ключевых компонентов, которые взаимодействуют между собой для обеспечения функциональности системы. Вот основные компоненты архитектуры Android:   1. **Ядро Linux:**    * Android базируется на ядре Linux, которое обеспечивает базовую функциональность операционной системы, включая управление процессами, управление памятью, обработку файловой системы, безопасность и драйверы устройств. 2. **Android Runtime (ART):**    * ART - это среда выполнения приложений для Android, которая запускает и выполняет приложения на устройстве. ART использует преобразование кода на уровне приложения (AOT) для повышения производительности и оптимизации использования ресурсов. 3. **Фреймворк приложений Android (Android Application Framework):**    * Этот фреймворк предоставляет набор API и инструментов разработки для создания приложений для Android. Он включает в себя различные компоненты, такие как активности (Activities), сервисы (Services), приемники широковещательных сообщений (Broadcast Receivers) и контент-провайдеры (Content Providers). 4. **Библиотеки Android (Android Libraries):**    * Android поставляется с набором стандартных библиотек, которые предоставляют различные функциональные возможности, такие как работа с графикой, мультимедиа, базами данных, сетевыми запросами и другими задачами. 5. **Android Системные приложения (Android System Apps):**    * Это предустановленные приложения, которые поставляются с операционной системой и предоставляют базовые функции, такие как управление контактами, отправка SMS, просмотр веб-страниц и другие. 6. **HAL (Hardware Abstraction Layer):**    * HAL предоставляет стандартизированный интерфейс для взаимодействия с аппаратным обеспечением устройства, что позволяет разработчикам создавать приложения, не зависящие от конкретной аппаратной платформы. 7. **Ядро Android (Android Kernel):**    * Этот компонент включает в себя дополнительные драйверы устройств и модули, специфичные для Android, такие как драйверы камеры, аудио и дисплея. 8. **Точки доступа к API:**    * Android предоставляет разработчикам доступ к широкому спектру API для создания приложений, использующих функциональные возможности устройства, такие как камера, датчики, GPS и другие   Формат структуры данных ASN.1. ASN.1 (Abstract Syntax Notation One) - это формат структуры данных, используемый для описания и кодирования структур данных в сетевых протоколах, таких как LDAP, SNMP, X.509 и других. Вот основные характеристики формата ASN.1:   1. **Абстрактный синтаксис:** ASN.1 предоставляет абстрактное описание структуры данных, независимо от конкретной реализации или языка программирования. 2. **Типы данных:** ASN.1 определяет различные типы данных, такие как целые числа, строки, последовательности, наборы и т. д. 3. **Описание данных:** С помощью ASN.1 можно описывать сложные структуры данных, включая их типы и вложенность. 4. **Независимость от платформы:** Формат ASN.1 обеспечивает переносимость данных между различными платформами и языками программирования. 5. **Кодирование данных:** ASN.1 определяет различные способы кодирования данных для их передачи по сети, включая BER (Basic Encoding Rules), DER (Distinguished Encoding Rules) и PER (Packed Encoding Rules). |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 22 |
| 1. Анализ угроз информационной безопасности. Классификация злоумышленников.   Анализ угроз информационной безопасности включает в себя идентификацию и оценку потенциальных угроз для информации, систем и ресурсов организации. Классификация злоумышленников помогает понять их мотивации, способы атак и цели, что в свою очередь помогает в разработке эффективных стратегий защиты. Вот основные категории злоумышленников:   1. **Хакеры (Hackers):**    * Хакеры могут быть как этичными, так и злонамеренными. Этичные хакеры (также известные как белые шляпы) используют свои навыки для тестирования безопасности систем и поиска уязвимостей для их исправления. Злонамеренные хакеры (черные шляпы) атакуют системы с целью получения несанкционированного доступа, кражи данных или нанесения ущерба. 2. **Киберпреступники (Cybercriminals):**    * Киберпреступники атакуют информационные системы с целью финансовой выгоды. Они могут взламывать банковские аккаунты, крадут личные данные для продажи на черном рынке или запрашивают выкуп за шифрованные данные (в случае атаки вымогателей). 3. **Шпионы (Spies):**    * Шпионы могут быть как государственными, так и корпоративными. Они атакуют системы с целью кражи конфиденциальной информации, технологических разработок, военных или политических секретов для использования в интересах своего правительства или организации. 4. **Активисты (Hacktivists):**    * Активисты используют технические средства для достижения политических или социальных целей. Они могут атаковать веб-сайты или системы в целях протеста, дефейса (взлома с целью изменения внешнего вида веб-сайта) или раскрытия информации. 5. **Сотрудники (Insiders):**    * Угроза информационной безопасности может исходить и изнутри самой организации. Внутренние злоумышленники могут использовать свой доступ к системам и данным для нанесения ущерба, кражи конфиденциальной информации или мошенничества. 6. **Непосредственные угрозы (Script Kiddies):**    * Это неопытные или неискусные злоумышленники, которые используют готовые инструменты и скрипты для проведения атак без необходимости в глубоких знаниях или навыках. 7. Базовые типы данных ASN.1 используемые в сертификате открытого ключа.   В сертификате открытого ключа (X.509) используются различные базовые типы данных ASN.1 для описания информации о сертификате и открытом ключе. Вот некоторые из основных типов данных ASN.1, которые используются в сертификатах открытых ключей:   1. **SEQUENCE и SET:**    * SEQUENCE и SET используются для определения последовательности или набора других типов данных. Например, в сертификате SEQUENCE используется для группировки различных полей сертификата. 2. **INTEGER:**    * INTEGER представляет целое число. В сертификатах открытых ключей INTEGER используется для представления различных числовых значений, таких как серийный номер сертификата или версия сертификата. 3. **OCTET STRING:**    * OCTET STRING представляет последовательность октетов, которая может использоваться для хранения бинарных данных. В сертификатах открытых ключей OCTET STRING часто используется для хранения открытого ключа, подписи и других бинарных данных. 4. **BOOLEAN:**    * BOOLEAN представляет логическое значение, которое может быть либо TRUE, либо FALSE. В сертификатах открытых ключей BOOLEAN используется для представления различных булевых свойств, таких как флаги доверия или активности сертификата. 5. **UTCTime и GeneralizedTime:**    * UTCTime и GeneralizedTime используются для представления временных меток в сертификатах открытых ключей. UTCTime используется для представления времени в формате UTC (Координированного всемирного времени), а GeneralizedTime позволяет представлять временные метки с большей точностью и гибкостью. 6. **OBJECT IDENTIFIER (OID):**    * OBJECT IDENTIFIER используется для представления уникального идентификатора объекта. В сертификатах открытых ключей OID используется для определения алгоритмов шифрования, хэширования и других параметров. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 23 |
| 1. Способы установки приложения на Android устройство.   Существует несколько способов установки приложений на устройства с операционной системой Android:   1. **Google Play Store:**    * Google Play Store является официальным магазином приложений для устройств на платформе Android. Пользователи могут найти и загрузить приложения из магазина, просматривая категории, используя поиск или следуя ссылкам на приложения. 2. **Сторонние магазины приложений:**    * В дополнение к Google Play Store существуют другие сторонние магазины приложений, такие как Amazon Appstore, Samsung Galaxy Store и другие. Они предлагают альтернативные источники для загрузки и установки приложений. 3. **Установка через файл APK:**    * Пользователи могут установить приложение, загрузив файл установочного пакета (APK) из Интернета или из другого источника, а затем запустив его на своем устройстве. Для этого необходимо разрешить установку из неизвестных источников в настройках безопасности устройства. 4. **Передача через USB или Bluetooth:**    * Пользователи могут передать файл установочного пакета (APK) на свое устройство с помощью USB-кабеля или Bluetooth соединения с другого устройства. 5. **Установка из хранилища файлов:**    * Пользователи могут сохранить файл установочного пакета (APK) в папке на устройстве, доступной через файловый менеджер, а затем запустить его на устройстве для установки. 6. **Автоматическая установка из других приложений:**    * Некоторые приложения могут предложить пользователю установить другие приложения, в том числе извне Google Play Store, например, через ссылки или рекомендации внутри приложения. 7. **Удаленная установка:**    * Пользователи могут установить приложения на свои устройства удаленно, используя функции управления устройством, такие как Google Play на веб-сайте, который позволяет выбрать устройство и установить приложения на него удаленно из браузера. 8. Структура каталога для хранения системных и пользовательских приложений.   В операционной системе Android приложения хранятся в специальных директориях на внутреннем хранилище устройства. Вот типичная структура каталогов для хранения системных и пользовательских приложений:   1. **Системные приложения:**    * /system/app/: В этой директории хранятся системные приложения, которые поставляются вместе с операционной системой. К ним относятся такие приложения, как камера, контакты, календарь и другие. Обычно доступ к этой директории имеют только системные процессы и приложения, поэтому обычному пользователю доступ к этой директории закрыт.    * /system/priv-app/: Аналогично директории /system/app/, здесь хранятся системные приложения, которые имеют особые привилегии доступа, например, доступ к основным функциям устройства. 2. **Пользовательские приложения:**    * /data/app/: В этой директории хранятся приложения, установленные пользователем из магазина приложений или вручную загруженные в формате APK. Каждому приложению обычно соответствует собственная поддиректория с именем пакета приложения.    * /data/data/: Здесь хранятся данные приложений, включая базы данных, настройки, кэши и другие файлы, используемые приложением во время его работы. Каждое приложение имеет свою собственную поддиректорию в /data/data/, и доступ к этой директории обычно имеет только само приложение. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 24 |
| 1. Компоненты и структура PKI.   PKI (Public Key Infrastructure) - это система, используемая для управления цифровыми сертификатами и ключами шифрования, предназначенная для обеспечения безопасности в сети. Вот основные компоненты и структура PKI:   1. **Центр сертификации (CA - Certification Authority):**    * CA является доверенным учреждением, которое выпускает и подписывает цифровые сертификаты. CA проверяет личность субъекта (владельца сертификата) и гарантирует связь между открытым ключом и идентификатором субъекта. 2. **Регистрационный центр (RA - Registration Authority):**    * RA выполняет процедуры аутентификации и регистрации пользователей перед передачей запросов на выдачу сертификатов CA. RA может выполнять проверку подлинности идентичности пользователей и сбор исходной информации для генерации сертификатов. 3. **Серверы доверенного хранения ключей (KMS - Key Management Servers):**    * KMS предоставляют инфраструктуру для генерации, хранения и управления ключами шифрования. Они обеспечивают безопасное хранение закрытых ключей и обеспечивают их доступность для цифровых подписей и шифрования. 4. **Субъекты (End Entities):**    * Субъектами являются пользователи или устройства, для которых выпускаются цифровые сертификаты. Субъекты могут быть лицами, серверами, программным обеспечением и другими сущностями, участвующими в обмене информацией в сети. 5. **Цифровые сертификаты:**    * Цифровые сертификаты содержат информацию о субъекте, его открытом ключе, сроке действия и информацию о CA, который выпустил сертификат. Они используются для проверки подлинности и обеспечивают безопасное шифрование и аутентификацию в сети. 6. **Цепочка сертификатов (Certificate Chain):**    * Цепочка сертификатов представляет собой иерархическую последовательность цифровых сертификатов, начиная от конечного сертификата и заканчивая корневым сертификатом CA. Она используется для проверки доверия сертификатам, начиная с конечного сертификата и заканчивая доверенным корневым сертификатом. 7. Классификация объектов информатизации по требованиям безопасности.   Классификация объектов информатизации по требованиям безопасности включает в себя разделение информации и информационных систем на различные уровни в соответствии с их значимостью и уровнем защиты, необходимым для обеспечения конфиденциальности, целостности и доступности данных. Вот основные категории классификации объектов информатизации по требованиям безопасности:   1. **Конфиденциальная информация:**    * Конфиденциальная информация относится к данным, доступ к которым ограничен и которые требуют дополнительной защиты для предотвращения несанкционированного доступа. Это могут быть персональные данные, коммерческая тайна, военная информация и другие конфиденциальные сведения. 2. **Секретная информация:**    * Секретная информация является подкатегорией конфиденциальной информации и обозначает данные с высоким уровнем секретности, доступ к которым строго регулируется и ограничивается. К ней могут относиться государственные секреты, военные тайны и другая критическая информация. 3. **Персональные данные:**    * Персональные данные относятся к информации, которая идентифицирует конкретного человека, такую как ФИО, адрес, номера телефонов, данные паспорта и другая личная информация. Защита персональных данных является особенно важной из-за рисков, связанных с нарушением конфиденциальности и права на неприкосновенность личной жизни. 4. **Критическая инфраструктура:**    * Критическая инфраструктура включает в себя системы и объекты, которые играют важную роль в обеспечении безопасности, экономики и общества в целом. Это могут быть энергетические сети, телекоммуникационные системы, финансовые институты и другие критические объекты. 5. **Общедоступная информация:**    * Общедоступная информация относится к данным, которые доступны для общего пользования и не требуют особых мер защиты. Это могут быть общедоступные документы, открытые данные, информация на сайтах государственных учреждений и другие публичные ресурсы. |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 25 |
| 1. Разделяемые сетевые ресурсы. NTFS и права доступа.   В Windows сетевые ресурсы могут быть разделены и управляться с помощью файловой системы NTFS (New Technology File System), которая поддерживает расширенные права доступа. Вот как NTFS и права доступа используются для управления разделяемыми сетевыми ресурсами:   1. **NTFS:**    * NTFS является файловой системой, используемой в операционных системах Windows. Она обеспечивает расширенные функции и возможности, такие как журналирование, шифрование, сжатие и аудит файлов. NTFS также поддерживает более гибкое управление правами доступа к файлам и папкам. 2. **Права доступа в NTFS:**    * В NTFS каждый файл и папка имеют набор разрешений, определяющих, кто может читать, записывать, исполнять или удалять их. Права доступа могут быть назначены как для отдельных пользователей и групп, так и для специальных системных аккаунтов.    * Основные права доступа в NTFS включают в себя:      + Чтение (Read): Разрешает просмотр содержимого файла или папки.      + Запись (Write): Разрешает создание, изменение и удаление файлов и папок.      + Исполнение (Execute): Разрешает выполнение исполняемых файлов (например, программ и скриптов).      + Полный доступ (Full Control): Предоставляет все вышеперечисленные права, а также право на изменение разрешений и владельца файла или папки.    * Права доступа можно назначать на уровне файлов и папок, а также на уровне дисков и томов. 3. **Управление разделяемыми сетевыми ресурсами:**    * Для управления доступом к разделяемым сетевым ресурсам в Windows можно использовать NTFS-права доступа в сочетании с настройками сетевых разрешений.    * Например, при создании сетевой папки на компьютере с Windows, вы можете указать, кто имеет доступ к этой папке и с какими правами. После этого NTFS-права доступа будут применяться к файлам и папкам внутри этой сетевой папки. 4. Механизмы внедрения динамических библиотек в процессы Windows.   Механизмы внедрения динамических библиотек (DLL) в процессы Windows предоставляют программам возможность использовать общие библиотеки кода, уменьшая дублирование кода и обеспечивая модульность и переиспользование. Вот основные способы внедрения DLL в процессы Windows:   1. **Явное связывание (Explicit Linking):**    * При явном связывании процесс программы явно загружает DLL-библиотеку и вызывает функции из неё, используя специальные функции, такие как LoadLibrary и GetProcAddress. Этот метод позволяет программе выбирать, когда и какая библиотека будет загружена, и дает большую гибкость в управлении процессом загрузки DLL. 2. **Неявное связывание (Implicit Linking):**    * При неявном связывании DLL-библиотеки загружаются автоматически при запуске программы. Система ищет и загружает необходимые DLL из определенных каталогов (например, каталог System32). Этот метод позволяет использовать функции из DLL, как если бы они были частью самой программы, без необходимости явного вызова функций загрузки. 3. **Загрузка DLL во время выполнения (Run-Time Dynamic Linking):**    * Этот подход сочетает в себе явное и неявное связывание. Программа может использовать функции загрузки DLL во время выполнения, чтобы динамически загружать и выгружать DLL в зависимости от потребностей программы. Например, функции LoadLibrary и FreeLibrary могут быть вызваны во время выполнения программы в зависимости от условий. 4. **DLL Injection (Внедрение DLL):**    * Внедрение DLL - это процесс вставки кода из DLL в адресное пространство процесса и последующего выполнения этого кода в контексте процесса. Этот метод часто используется для расширения функциональности программы или для внедрения кода злоумышленниками. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 26 |
| 1. Использование механизма Intent для расширения прав приложения.   Механизм Intent в Android используется для передачи данных между компонентами приложения (например, между активностью и службой) или между различными приложениями. Однако неправильное использование механизма Intent может привести к небезопасному расширению прав приложения. Вот несколько сценариев, когда механизм Intent может быть использован для расширения прав приложения:   1. **Использование неправильного намерения (Intent) для запуска действий:**    * Если приложение принимает неправильно настроенные Intent-фильтры, злоумышленник может запустить опасные действия, такие как отправка SMS или вызов дорогостоящих телефонных номеров, что может привести к несанкционированным действиям и расходам. 2. **Получение данных из других приложений без проверки их безопасности:**    * Если приложение использует Intent для получения данных из других приложений, оно должно проверять их подлинность и безопасность перед обработкой. В противном случае злоумышленник может передать поддельные данные или вредоносный контент, что может привести к утечке информации или атакам на приложение. 3. **Открытие активностей с небезопасными флагами:**    * Если активности приложения открываются с неправильно настроенными флагами Intent, это может привести к уязвимостям безопасности. Например, использование флага FLAG\_ACTIVITY\_CLEAR\_TASK может позволить злоумышленнику получить доступ к активности без авторизации.   Чтобы предотвратить небезопасное расширение прав приложения через механизм Intent, разработчики должны следовать рекомендациям по безопасному использованию Intents, таким как:   * Правильно настраивать Intent-фильтры с ограниченным набором действий и категорий. * Проверять подлинность и безопасность данных, получаемых через Intent. * Использовать безопасные флаги для открытия активностей и сервисов. * Ограничивать доступ к чувствительным данным и функциям приложения через механизмы аутентификации и авторизации.   Эти меры помогут обеспечить безопасное использование механизма Intent и предотвратить расширение прав приложения.   1. Система менеджмента информационной безопасности.   Система управления информационной безопасностью (Information Security Management System, ISMS) - это фреймворк, используемый организациями для управления и обеспечения безопасности информации в их деятельности. Основной стандарт для ISMS - это ISO/IEC 27001:2013. Вот ключевые элементы системы управления информационной безопасностью:   1. **Политика информационной безопасности:**    * Политика информационной безопасности определяет общие принципы и цели безопасности информации в организации. Она устанавливает обязательства руководства по обеспечению безопасности информации и создает основу для разработки конкретных правил и процедур. 2. **Риск-анализ и управление рисками:**    * ISMS включает в себя процесс анализа и оценки рисков для идентификации угроз, уязвимостей и потенциальных последствий нарушений безопасности. На основе этого анализа разрабатываются меры по снижению и управлению рисками. 3. **Управление активами:**    * ISMS включает в себя управление информационными активами организации, такими как данные, программное обеспечение, оборудование и интеллектуальная собственность. Это включает в себя идентификацию активов, их классификацию и защиту в соответствии с их значимостью и чувствительностью. 4. **Безопасность операций:**    * ISMS включает в себя управление безопасностью операций, включая защиту информации в процессе обработки, передачи и хранения. Это включает в себя управление доступом, защиту сетей, мониторинг и обнаружение инцидентов, а также управление изменениями. 5. **Управление обеспечением:**    * ISMS включает в себя управление поставщиками и сторонними поставщиками услуг, чтобы обеспечить безопасность информации внутри и вне организации. Это включает в себя оценку безопасности поставщиков, заключение договоров о безопасности и мониторинг исполнения обязательств. 6. **Мониторинг и улучшение:**    * ISMS включает в себя процессы мониторинга эффективности системы, обнаружения инцидентов безопасности и улучшения процессов безопасности на основе выявленных недостатков и опыта. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 27 |
| 1. Способы установки приложения на Android устройство.   На устройствах Android приложения могут быть установлены несколькими способами:   1. **Установка из Google Play Store:**    * Google Play Store является официальным магазином приложений для устройств Android. Пользователи могут просто перейти в Google Play Store, найти нужное приложение с помощью поиска или просмотреть категории, выбрать приложение и нажать кнопку "Установить". После этого приложение будет загружено и автоматически установлено на устройство. 2. **Установка из других магазинов приложений:**    * Помимо Google Play Store, существуют и другие магазины приложений для Android, такие как Amazon Appstore, Samsung Galaxy Store и другие. Пользователи могут установить эти магазины и искать и устанавливать приложения через них. 3. **Установка из файлов .apk:**    * Пользователи могут устанавливать приложения, загруженные в формате .apk (Android Package), напрямую на устройство, обходя магазины приложений. Для этого необходимо скачать файл .apk с интернета или другого источника на устройство, а затем открыть его с помощью файлового менеджера или другого приложения для установки. Важно помнить, что установка приложений из неизвестных источников может быть опасной и не рекомендуется безопасности вашего устройства. 4. **Установка через компьютер:**    * Приложения также могут быть установлены на устройство с помощью компьютера. Это может быть сделано через официальный веб-сайт разработчика приложения или с помощью специального программного обеспечения для управления устройством. 5. Структура каталога для хранения системных и пользовательских приложений.   В операционной системе Android приложения хранятся в специальной структуре каталогов в файловой системе устройства. Вот основная структура каталогов для хранения системных и пользовательских приложений:   1. **/system/app/:**    * В этом каталоге хранятся системные приложения, которые поставляются вместе с операционной системой Android. Обычно доступ к этому каталогу имеют только системные процессы. 2. **/data/app/:**    * Этот каталог содержит пользовательские приложения, установленные на устройстве. Каждое приложение обычно представлено отдельной папкой с именем, соответствующим пакетному имени приложения. 3. **/data/data/:**    * В этом каталоге хранятся данные приложений, такие как настройки, кэш, базы данных и другие файлы, связанные с работой приложений. Каждое приложение имеет свой собственный подкаталог с именем, соответствующим пакетному имени приложения. 4. **/sdcard/Android/data/:**    * Этот каталог используется для хранения данных приложений на внешнем устройстве хранения (например, на карте памяти SD). Подкаталоги в этой директории соответствуют пакетным именам приложений и содержат данные, которые приложения могут сохранять на внешнем хранилище. 5. **/sdcard/Android/obb/:**    * В этом каталоге хранятся дополнительные файлы данных приложений (например, файлы данных игр), которые могут быть слишком большими для включения в основное приложение. Этот каталог также располагается на внешнем устройстве хранения. |
|  |
|  |

|  |
| --- |
| Экзаменационный билет № 28 |
| 1. Сертификат открытого ключа. Назначения. Основные поля.   Сертификат открытого ключа (Certificate) - это электронный документ, который привязывает открытый ключ к субъекту (например, веб-сайту, организации или пользователю) и утверждает его подлинность. Сертификаты открытого ключа широко используются в криптографии и сетевой безопасности для обеспечения конфиденциальности, целостности и аутентификации в сетевых коммуникациях. Вот основные назначения и поля сертификата открытого ключа:  **Назначения:**   1. **Аутентификация:** Сертификаты открытого ключа используются для проверки подлинности субъекта, то есть для убеждения в том, что субъект является тем, за кого он себя выдаёт. 2. **Шифрование:** Сертификаты открытого ключа могут использоваться для шифрования секретной информации с использованием открытого ключа получателя, что обеспечивает конфиденциальность сообщений. 3. **Цифровая подпись:** Сертификаты открытого ключа позволяют создавать и верифицировать цифровые подписи, которые утверждают подлинность и целостность документов и сообщений.   **Основные поля:**   1. **Субъект (Subject):** Это информация о сущности, к которой привязан сертификат, например, название организации или URL веб-сайта. 2. **Отпечаток (Thumbprint):** Это уникальный хэш-значение сертификата, используемое для его идентификации. 3. **Открытый ключ (Public Key):** Это сам открытый ключ, который привязан к сертификату и используется для шифрования данных или проверки подписей. 4. **Идентификатор алгоритма подписи (Signature Algorithm):** Это алгоритм, который использовался для создания цифровой подписи сертификата. 5. **Истекаемость (Validity Period):** Это временной период, в течение которого сертификат считается действительным. 6. **Издатель (Issuer):** Это сущность, которая выпустила (подписала) сертификат и подтверждает его подлинность. 7. **Расширения (Extensions):** Это дополнительные поля, которые могут содержать дополнительную информацию, такую как названия дополнительных субъектов или ограничения использования сертификата 8. Политика информационной безопасности.   Политика информационной безопасности (ПИБ) - это документ, который определяет принципы, правила, процедуры и практики, направленные на обеспечение безопасности информации в организации. ПИБ является ключевым компонентом системы управления информационной безопасностью (СУИБ) и служит основой для разработки и реализации мер по защите информации. Вот основные аспекты политики информационной безопасности:   1. **Цели и принципы:** ПИБ определяет цели и принципы обеспечения безопасности информации в организации, которые могут включать конфиденциальность, целостность, доступность, аутентификацию, а также принципы неотвратимости и разумности. 2. **Область применения:** ПИБ устанавливает область применения, к которой применяются её положения, включая информацию, системы, процессы и людей, находящихся в пределах организации. 3. **Роли и обязанности:** ПИБ определяет роли и обязанности сотрудников и других заинтересованных лиц в обеспечении безопасности информации, включая управление рисками, управление доступом, обучение и обучение персонала, мониторинг и реагирование на инциденты. 4. **Положения и правила:** ПИБ содержит положения и правила, которые определяют ожидаемое поведение персонала и других пользователей информационных ресурсов, включая использование паролей, шифрование данных, обработку конфиденциальной информации и другие аспекты безопасности. 5. **Меры безопасности:** ПИБ устанавливает меры безопасности, которые должны быть приняты для защиты информации, включая технические, организационные и процедурные меры, такие как установка антивирусного программного обеспечения, регулярное обновление программного обеспечения, установка брандмауэров и другие. 6. **Обучение и осведомленность:** ПИБ включает требования по обучению и осведомленности персонала по вопросам информационной безопасности, чтобы персонал был знаком с политиками, процедурами и мерами безопасности, и мог активно участвовать в обеспечении безопасности информации. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 29 |
| 1. Атаки на DNS сервисы.   Атаки на DNS (Domain Name System) сервисы могут иметь серьезные последствия для работы сети и безопасности информации. Вот несколько типичных атак на DNS:   1. **DNS Spoofing (DNS Cache Poisoning):** Это атака, при которой злоумышленник вводит ложные данные в кэш DNS сервера или клиента, например, подменяя IP-адреса для доменных имен. Это может привести к перенаправлению пользователей на фальшивые веб-сайты или использованию фальшивых серверов. 2. **DNS Amplification Attack:** В этом типе атаки злоумышленник отправляет запросы на открытые рефлекторы DNS с поддельным IP-адресом жертвы. Это приводит к тому, что DNS серверы отправляют большие объемы данных на жертву, что может вызвать отказ в обслуживании (DDoS). 3. **DNS Tunneling:** Это метод использования DNS протокола для передачи нежелательного трафика или обхода ограничений безопасности. Злоумышленник может использовать DNS запросы и ответы для передачи данных между компрометированным устройством и удаленным сервером. 4. **DNS Hijacking:** В этой атаке злоумышленник перехватывает DNS запросы и направляет их на свои фальшивые серверы DNS. Это позволяет злоумышленнику перенаправлять пользователей на фальшивые веб-сайты или перехватывать учетные данные. 5. **Denial of Service (DoS) Attack:** Это атака, при которой злоумышленник затопляет целевой DNS сервер или сеть DNS запросами, что приводит к перегрузке и недоступности сервиса для легальных пользователей 6. Требования по сертификации средств защиты информации.   Сертификация средств защиты информации является важным процессом, который подтверждает соответствие этих средств определенным стандартам и требованиям безопасности. В различных странах могут существовать различные программы сертификации, но общие требования могут включать в себя следующее:   1. **Стандарты безопасности:** Средства защиты информации должны соответствовать определенным стандартам безопасности, таким как ISO 27001, Common Criteria (CC), FIPS (Federal Information Processing Standards) и другие. 2. **Алгоритмы и протоколы:** Продукты должны использовать алгоритмы и протоколы, которые признаны надежными и безопасными, такие как алгоритмы шифрования, протоколы аутентификации и т. д. 3. **Проверенные методы и процессы разработки:** Разработка и производство средств защиты информации должны осуществляться с использованием проверенных методов и процессов, направленных на обеспечение безопасности и качества продукта. 4. **Тестирование и аудит:** Средства защиты информации должны проходить тщательное тестирование безопасности и аудиты, чтобы убедиться в их надежности и соответствии стандартам безопасности. 5. **Документация и отчетность:** Процесс сертификации должен включать в себя подготовку документации и отчетов о безопасности продукта, включая описание функций безопасности, результаты тестирования и другую информацию. 6. **Адекватность защиты:** Продукты должны обеспечивать адекватный уровень защиты информации, соответствующий рисковому профилю организации и требованиям безопасности. 7. **Сертификация производителя:** В некоторых случаях может потребоваться сертификация самого производителя средств защиты информации, чтобы подтвердить их способность разрабатывать безопасные продукты и обеспечивать поддержку и обновления. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 30 |
| 1. Атаки на ARP протокол.   ARP (Address Resolution Protocol) - это протокол, используемый в компьютерных сетях для преобразования IP-адресов в MAC-адреса (и наоборот), чтобы устройства могли общаться друг с другом в локальной сети. Атаки на ARP могут представлять серьезную угрозу для безопасности сети. Вот несколько типов атак на ARP:   1. **ARP Spoofing (ARP Cache Poisoning):** Это один из наиболее распространенных видов атак на ARP. Злоумышленник отправляет ложные ARP ответы на устройства в сети, утверждая, что его MAC-адрес является MAC-адресом другого устройства (например, шлюза). Это позволяет злоумышленнику перехватывать или перенаправлять сетевой трафик, включая чувствительные данные. 2. **ARP Poison Routing:** В этой атаке злоумышленник отправляет ложные ARP ответы, но вместо того, чтобы перенаправлять трафик, он просто переправляет трафик через свою собственную машину, где он может быть перехвачен или изменен, прежде чем достигнет его истинного назначения. 3. **ARP Flood Attack:** В этой атаке злоумышленник отправляет огромное количество ложных ARP запросов или ответов в сеть, что приводит к перегрузке и отказу в обслуживании (DoS) на целевых устройствах или сети в целом. 4. **Man-in-the-Middle (MITM) Attack:** ARP атаки могут использоваться в рамках атаки Man-in-the-Middle, когда злоумышленник перехватывает и манипулирует сетевым трафиком между двумя устройствами, внося изменения или подслушивая чувствительные данные. 5. **ARP Router Advertisement Spoofing:** Злоумышленник может отправлять ложные ARP сообщения о маршрутизаторе (Router Advertisement), чтобы заставить устройства в сети использовать его фальшивый маршрутизатор, что позволяет ему контролировать или перехватывать сетевой трафик. 6. Методы защиты личных ключей шифрования и ЭЦП.   Защита личных ключей шифрования и ЭЦП (электронной цифровой подписи) критически важна для обеспечения безопасности информации и подтверждения её подлинности. Вот несколько методов защиты личных ключей:   1. **Хранение на защищенных носителях:** Личные ключи могут храниться на защищенных носителях, таких как смарт-карты, USB-токены или аппаратные модули безопасности (HSM). Эти устройства обычно обеспечивают аппаратную защиту ключей и могут быть защищены паролем, биометрическими данными или другими методами аутентификации. 2. **Шифрование ключей:** Личные ключи могут быть зашифрованы с использованием дополнительного пароля или другого секрета. При использовании ключа, пользователь должен будет предоставить этот пароль или секрет для дешифровки ключа перед его использованием. 3. **Многофакторная аутентификация:** Для доступа к личным ключам может использоваться многофакторная аутентификация, такая как сочетание пароля и физического токена, биометрических данных и т. д. Это повышает уровень безопасности и защищает ключи от несанкционированного доступа. 4. **Ограниченный доступ:** Личные ключи должны иметь ограниченный доступ только для авторизованных пользователей или процессов. Это может быть достигнуто с помощью систем управления доступом, таких как ACL (списки контроля доступа) или RBAC (ролевой доступ). 5. **Регулярная смена ключей:** Для уменьшения риска компрометации личных ключей рекомендуется периодически менять их. Это позволяет сократить время, в течение которого злоумышленник может использовать компрометированный ключ. 6. **Мониторинг и аудит:** Необходимо вести мониторинг и аудит действий, связанных с использованием личных ключей, чтобы обнаружить подозрительную активность и реагировать на неё. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 31 |
| 1. Запрос на выпуск сертификата открытого ключа. Назначение. Основные поля.   Запрос на выпуск сертификата открытого ключа (Certificate Signing Request, CSR) представляет собой файл, создаваемый владельцем ключа (например, сервером или пользователем), который запрашивает организацию выпустить сертификат для их открытого ключа. Назначение CSR заключается в предоставлении данных, необходимых для создания цифрового сертификата, который затем может использоваться для аутентификации и шифрования данных.  Основные поля, обычно содержащиеся в CSR, включают следующие:   1. **Идентификатор субъекта (Subject):** Это информация о лице или организации, для которой выпускается сертификат. Обычно включает в себя такие данные, как имя организации, страна, штат (регион), город, фамилия, имя и адрес электронной почты. 2. **Открытый ключ (Public Key):** Это открытый ключ, для которого запрашивается сертификат. Он используется для шифрования данных и/или проверки подписей. 3. **Алгоритм подписи (Signature Algorithm):** Это алгоритм, используемый для создания цифровой подписи CSR. Например, может быть использован RSA, DSA или ECDSA. 4. **Дополнительные атрибуты (Extensions):** Это дополнительные атрибуты, которые могут быть включены в CSR, такие как информация о расширениях ключа или атрибуты, связанные с определенным протоколом или приложением. 5. **Идентификатор запроса (Request Identifier):** Уникальный идентификатор, который может быть использован для отслеживания запроса сертификата. 6. **Другие данные (Additional Data):** В CSR также может быть включена дополнительная информация, такая как информация о сертификате, которую хочет получить владелец ключа, или другие сведения о целях использования сертификата. 7. Средства обеспечения подлинности данных.   Средства обеспечения подлинности данных используются для проверки целостности и подлинности информации. Вот несколько распространенных методов обеспечения подлинности данных:   1. **Хэш-функции:** Хэш-функции используются для создания уникального "отпечатка" или "хэша" исходных данных. Этот хэш затем может быть использован для проверки целостности данных. Даже небольшое изменение в исходных данных приведет к значительному изменению хэша. 2. **Цифровые подписи:** Цифровые подписи используются для подтверждения подлинности данных и идентификации отправителя. Это достигается путем шифрования хэша данных с использованием частного ключа отправителя. Получатель может затем расшифровать хэш с использованием общедоступного ключа отправителя и сравнить его с вычисленным хэшем полученных данных для проверки подлинности и целостности. 3. **Сертификаты цифровых подписей:** Сертификаты цифровых подписей используются для проверки подлинности открытого ключа, используемого для проверки подписей. Эти сертификаты предоставляют доверенную сторону, которая утверждает, что открытый ключ принадлежит указанному отправителю. 4. **MAC (Message Authentication Code):** MAC используется для проверки целостности и подлинности данных, используя секретный ключ. MAC создается путем применения алгоритма хэширования к сообщению с использованием секретного ключа. Получатель затем может вычислить MAC и сравнить его с полученным для проверки целостности и подлинности данных. 5. **Блокирование (Sealing):** Блокирование - это процесс привязки данных к определенному контексту или среде, что обеспечивает дополнительный уровень подлинности и защиты данных от изменений или вмешательства. |
|  |
|  |

|  |
| --- |
|  |
| Экзаменационный билет № 32 |
| 1. Атаки на технологию электронной цифровой подписи.   Технология электронной цифровой подписи (ЭЦП) обеспечивает аутентификацию и целостность электронных документов путем использования математических алгоритмов для создания и проверки цифровых подписей. Однако она также подвержена различным атакам и угрозам. Вот некоторые типы атак, связанные с технологией ЭЦП:   1. **Фальсификация ключей:** Атаки, направленные на подмену легитимного открытого ключа поддельным ключом злоумышленника. Это может позволить злоумышленнику создавать поддельные цифровые подписи, подделывая подлинность данных. 2. **Компрометация закрытого ключа:** Если закрытый ключ, используемый для создания цифровой подписи, станет известным злоумышленнику, это может привести к созданию поддельных подписей от имени владельца ключа. 3. **Атаки методом перебора:** Атаки, включающие попытки подбора закрытого ключа методом перебора или другими методами криптоанализа. Чем слабее ключ, тем больше вероятность его взлома. 4. **Социальная инженерия:** Атаки, направленные на убеждение владельца ключа в разглашении своего закрытого ключа или выполнении подписи на фальшивых данных. 5. **Отказ в обслуживании (DoS):** Атаки, направленные на перегрузку или нарушение работы системы проверки подписей, что может привести к невозможности аутентификации и целостности электронных документов. 6. **Использование уязвимостей в алгоритмах подписи:** Уязвимости, обнаруженные в алгоритмах подписи, могут быть использованы злоумышленниками для создания поддельных подписей или обхода проверки подлинности. 7. **Внедрение вредоносного программного обеспечения:** Вредоносное программное обеспечение, установленное на компьютер владельца ключа, может перехватывать или модифицировать процесс создания или проверки цифровых подписей.   Для защиты от атак на технологию ЭЦП необходимо использовать сильные криптографические алгоритмы, безопасное хранение закрытых ключей, механизмы аутентификации владельца ключа, а также мониторинг и обновление системы подписи для устранения уязвимостей. Кроме того, обучение пользователей основным принципам безопасности и предупреждение о социальной инженерии также играют важную роль в защите от атак на технологию ЭЦП.   1. Принцип работы OCSP-сервиса. |
| OCSP (Online Certificate Status Protocol) - это протокол, который используется для проверки статуса действительности цифрового сертификата. Принцип работы OCSP-сервиса включает следующие шаги:   1. **Запрос на проверку статуса сертификата:** Когда приложение или система требует проверки статуса цифрового сертификата, оно отправляет запрос OCSP на OCSP-сервер. 2. **Запрос OCSP-сервера:** OCSP-сервер получает запрос на проверку статуса сертификата и анализирует его. Затем сервер проверяет свойства сертификата, указанные в запросе. 3. **Получение статуса сертификата:** После анализа запроса OCSP-сервер проверяет, является ли сертификат действительным, отозванным или находится в другом статусе. Для этого сервер использует информацию из своей базы данных статусов сертификатов. 4. **Ответ OCSP-сервера:** После проверки OCSP-сервер отправляет ответ на запрос, который содержит информацию о статусе сертификата. Этот ответ может быть положительным (сертификат действителен), отрицательным (сертификат отозван) или другим, в зависимости от результата проверки. 5. **Обработка ответа клиентом:** Приложение или система, отправившая запрос, получает ответ от OCSP-сервера. Затем она обрабатывает этот ответ и принимает соответствующие действия в зависимости от статуса сертификата. Например, если сертификат отозван, приложение может отказать в доступе к ресурсам, защищенным этим сертификатом. |
|  |