1. Классификация методов защиты информации.   
   Классификация: правовые, организационные, инженерные (технические, информационные, физические)
2. Классификация методов защиты информации: административные и ограничительные
3. Организационно-административные методы защиты информации - комплекс административных и ограничительных мер, направленных на защиту информации путем регламентации деятельности персонала и порядка функционирования средств (систем).
4. Состав организационно-распорядительных документов – перечень информации, подлежащий защите; документы, регламентирующие порядок обращения к защищённым данным; положения о структурных подразделениях предприятия; док-ты, регламентирующие взаим. предприятия со сторонними организациями по вопросам обмена информацией; док-ты, регламентирующие порядок эксплуатации автоматизированных систем предприятия; планы защиты автоматизированных систем предприятия; док-ты, регламентирующие порядок разработки, испытания и сдачи в экспл. ПО; док-ты, реглам. порядок закупки программных и аппаратных средств; док-ты, регламентирующие порядок эксплуатации техн. Средств связи и телекоммуникации.
5. Что должна содержать маркировка носителей информации? Учётный номер, гриф секр, подпись, присвоенным владельцем сертификата.
6. Кто отвечает за соблюдение в организации организационных мер? На руководителе, начальнике службы безопасности (информационной безопасности), системном (сетевом) администраторе
7. Что такое «Политика безопасности». Совокупность документированных управленческих решении, направленных на защиту информации и ассоциированных с ней ресурсов.
8. Базовая политика безопасности. В ней определяются разрешенные и запрещенные действия, а также указываются необходимые средства управления в рамках реализуемой архитектуры безопасности.
9. Понятие специализированных политик безопасности. Специализированные политики безопасности затрагивают значительное число пользователей или связаны с конкретными техническими областями. (прим: политика удалённого доступа)
10. Политика безопасности допустимого использования устанавливает стандартные нормы безопасного использования компьютерного оборудования и сервисов в компании, а также соответствующих мер безопасности сотрудников для защиты корпоративных ресурсов и собственной информации.
11. Политика удаленного доступа устанавливает стандартные нормы безопасного удалённого соединения любого хоста с сетью компании.
12. Понятие процедур безопасности. Определяют, как защитить ресурсы и каковы механизмы выполнения политики, т. е. как реализовывать политики безопасности.
13. Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ.
14. Принцип минимизации привилегий принцип организации доступа к ресурсам, когда в тот или иной уровень абстракции от вычислительной среды, каждый модуль (такой, как процесс, пользователь или программа, которые мы рассматриваем) должны иметь доступ к такой информации и ресурсам, которые минимально необходимы для успешного выполнения его рабочей цели.
15. Принцип разделения обязанностей. (можно пинать хуй) ни один участник труда не имеет единоличного контроля над производством или заданием.
16. Принцип эшелонированности обороны. это подход, который предполагает разделение информационной системы на несколько «эшелонов», каждый из которых имеет свои собственные меры безопасности. Короче, система защиты в несколько уровней.
17. Принцип разнообразия защитных средств. Предполагает создание различных по своему характеру оборонительных рубежей, чтобы от потенциального злоумышленника требовалось овладение разнообразными техническими средствами.
18. Принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только в простой системе можно проверить её работоспособность и слаженность механизмов, поэтому она должна быть простой в управлении.
19. Принцип всеобщей поддержки мер безопасности. Поддерживать меры безопасности обязан каждый сотрудник без исключения.
20. Принцип адекватности. От всего защититься не получится, Методы защиты должны быть дифференцированы в зависимости от важности, частоты и вероятности возникновения угроз информационной безопасности. Для наименее важных можно принять риск.
21. Системность. Предполагает взаимосвязь процессов организации защиты информационных ресурсов, согласованное применение методов и средств защиты информационных ресурсов.
22. Прозрачность для легальных пользователей. Не усложнять слишком сильно доступ к ресурсу реальных пользователей (пример: <https://neal.fun/password-game/>)
23. Равностойкость звеньев. Прочность системы обозначается стойкостью самого слабого звена. Увеличил стойкость одного звена в целом система стойкость не повысит. Поэтому все звенья защиты должны быть одинаково стойки.
24. Главные этапы построения политики безопасности:
    1. обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
    2. выбор и установка средств защиты;
    3. подготовка персонала работе со средствами защиты;
    4. организация обслуживания по вопросам информационной безопасности;
    5. создание системы периодического контроля информационной безопасности ИС.

Определения сами допишите!

<https://studfile.net/preview/16707525/page:8/>

РУОИДНА ЛТЬБЯ