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. 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.
11. 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.
12. Принцип разделения обязанностей. (можно пинать хуй) ни один участник труда не имеет единоличного контроля над производством или заданием.
13. 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.
14. Принцип разнообразия защитных средств. Предполагает создание различных по своему характеру оборонительных рубежей, чтобы от потенциального злоумышленника требовалось овладение разнообразными техническими средствами.
15. Принцип всеобщей поддержки мер безопасности. Поддерживать меры безопасности обязан каждый сотрудник без исключения.
16. 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.
17. Системность. Предполагает взаимосвязь процессов организации защиты информационных ресурсов, согласованное применение методов и средств защиты информационных ресурсов.
18. Прозрачность для легальных пользователей. Не усложнять слишком сильно доступ к ресурсу реальных пользователей (пример: <https://neal.fun/password-game/>)
19. 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.
20. 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.
21. Объект информатизации — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов, в которых они установлены, а также помещения и объекты для ведения конфиденциальных разговоров. Примеры: принтеры, сервера, компьютеры, сигнализация, средства в помещении с компом и т. д.
22. Аттестация — комплекс организационно-технических мероприятий, в результате которых посредством специального документа «Аттестат соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утверждённых ФСТЭК.Наличие аттестата соответствия в организации даёт право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в аттестате.
23. Согласно приказу №77, срок проведения работ по аттестации объекта информатизации устанавливается владельцем объекта информатизации по согласованию с органом по аттестации, но не может превышать четырех месяцев.
24. Аттестации обязательно подлежат государственные и муниципальные информационные системы, информационные системы управления военного производства, помещения для конфиденциальных переговоров. Необязательной аттестации подлежат критическая информационная структура, информационные средства с персональными данными, потенциально опасные объекты
25. Согласно приказу №77, Владелец ОИ должен не реже одного раза в 2 года предоставлять протоколы контроля защиты информации на аттестованном ОИ в ФСТЭК России (территориальный орган ФСТЭК России).
26. Дополнительные испытания и повторная аттестация проводится при исключении программных, программно-технических средств и средств защиты информации, дополнительно включены аналогичные средства или заменены ына аналогичные средства, в случае развития (модернизации) ОИ, приводящего к повышению класса защищенности (уровня защищенности, категории значимости) ОИ и (или) к изменению архитектуры системы защиты информации ОИ в части изменения видов и типов программных, программно-технических средств и средств защиты информации, изменения структуры системы защиты информации, состава и мест расположения ОИ и его компонентов.

Определения сами допишите!

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

РУОИДНА ЛТЬБЯ