1. Безопасность автоматизированной системы — состояние автоматизированной системы, определяющее защищённость обрабатываемой информации и ресурсов системы от деструктивных воздействий, называемых угрозами, а также способность автоматизированной системы выполнять предписанные функции.
2. Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую систему.
3. Система защиты информации в автоматизированной системе — меры правового, организационного, технического (физического, информационно-технологического, криптографического), специального характера и также соответствующие им мероприятия.
4. Политика информационной безопасности — совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которыми руководствуется организация в своей деятельности
5. Основные защитные меры
   1. Подсистема управления доступом
      1. Идентификация пользователей
      2. Идентификация ЭВМ, устройств, программ
      3. Контроль доступа субъектов к защищаемым ресурсам
      4. Управление потоками информации с помощью меток конфиденциальности
   2. Подсистема регистрации и учёта
      1. Регистрация входа (и выхода) пользователей в систему
      2. Регистрация запуска/завершения программ и процессов
      3. Регистрация доступа программ пользователей к защищаемым файлам
      4. Регистрация попыток доступа
      5. Регистрация изменения полномочий пользователя
      6. Учёт защищаемых носителей информации
      7. Очистка освобождённых областей ОЗУ
      8. Сигнализация попыток нарушения защиты
   3. Криптографическая защита
      1. Шифрованиие всей конфи
      2. Контроль доступа пользователей к операциям шифрования и доступа к криптографическим ключам
      3. Использование разных криптографических ключей
   4. Обеспечения целостности
      1. Проверка целостности программных средств СЗИ НСД, обрабатываемой информациои, неизменность программной среды
      2. Физическая охрана средств вычислительной техники и носителей информации
      3. Периодическое тестирование СЗИ от НСД
      4. Наличие средств восстановления СЗИ от НСД
   5. Подсистема антивирусной защиты
      1. Блокировка вирусных воздействий на системные области, ПО
      2. Контроль целостной файловой системы
      3. Обнаружение вирусов в архивах
      4. Удаление обнаруженных вирусов
      5. Самоконтроль целостности
6. Средства защиты информации — технические, криптографические, программные и другие средства, предназначенные для реализации совокупности взаимосвязанных требований безопасности автоматизированной системы, а также средства контроля эффективности защиты информации
7. Классы СЗИ
   1. Средства защиты НСД
   2. Средства криптографической защиты
   3. Средства сетевого воздействия
8. Ещё одна классификация программно-аппаратное средство защиты информации от НСД?
   1. Система управления доступом
      1. Подсистема доверенной загрузки
      2. Подсистема идентификации и аутентификации
      3. Подсистема контроля целостности системного ПО
      4. Подсистема разграничения доступа
      5. Подсистема замкнутой программной среды
   2. Система регистрации и контроля критичных событий
   3. Система контроля целостности данных
   4. Система криптографической защиты
      1. Подсистема сетевой защиты
      2. Подсистема кничтожения остаточной информации
      3. Подсистема шифрования данных
      4. Открытый интерфейс подсистемы криптозащиты
9. Основные функции СЗИ (Страж NT, Dallas Lock, Secret NET 5.0-C, Аккорд-NT/2000)
   1. организация доверенной загрузки с возможностью идентификации и аутентификации пользователей при помощи ключевых носителей информации, включая авторизация пользователей во временной области
   2. Контроль целостности системных областей жёсткого диска, назначенных администратором безопасности системы
   3. Контроль целостности конфигурации аппаратныхх средств
   4. Регистрация событий доступа в ПЗУ
10. Дополнительные функции
    1. Дискреционная и мандатная модели разграничения доступа (мандатная — пользователи не могут управлять настройками политик безопасности, дискреционная — могут, прим — разграничение доступа к фалам на линуксе)
    2. Создание для пользователей замкнутой программной среды
    3. Контроль потоков защищаемой информации
    4. Очистка освобождаемой памяти и дискового пространства
    5. Аудит доступа к защищаемым ресурсам
    6. Управление вводом выводом на отчуждаемые носители
11. Критическая информационная инфраструктура — ИС, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия.
12. Субъекты КИИ — компании, работающие в стратегически важных для государства областях, таких как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно энергетический комплекс, в области атомной энергии, оборонной, ракетно космической, горнодобывающей, металургической и химической промышленности, а также организации, обеспечивающие взаимодействие систем или сетей КИИ
13. SOC (Security Operations Center) или CSOC — центр мониторинга кибербезопасности
14. SOC — группа специалистов по защите информации, которые непрерывно осуществляют контроль за сообщениями, поступающими от технических средств, для того, чтобы как можно оперативнее устранить угрозу ИБ
15. Основная задача SOC — обеспечение реагирования на инциденты информационной безопасности в рамках заранее согласованного соглашение о качестве оказываемых услуг.