Защита неструктурированных данных: проблемы, подходы и инструменты для их решения

- Проблематика
  - Цели злоумышленников
    - Кража данных
    - Порча данных
      - Резервное копирование
        - Специализированные инструменты и ПО
        - Ресурсы для хранения данных
          - Локальная файловая система
          - Публичные или приватные облака
          - Внешние хранилища
          - Почтовые сервисы
  - Подходы и инструменты для хранения и защиты неструктурированных данных в операционных системах
    - Пользовательские ОС
      - Windows, Linux, MacOS
      - ОС для мобильных устройств
        - Проблемы мониторинга СЗИ
    - Серверные ОС и специализированные инструменты для управления файловыми хранилищами
    - Компетенции пользователей и администраторов в части защиты неструктурированных данных
      - Пользователи
        - Понимание принципов работы общего доступа к папкам и файлам
        - Полномочия для назначения прав на папки и файлы
        - Культура структурирования пользовательских данных
        - Данные приложений
          - Временные файлы
          - Выбор директорий для сохранения файлов из приложений
      - Администраторы
        - Понимание бизнес-процессов и контроль потоков данных
        - Уступчивость
        - Компетенции в области ИБ
    - Кибергигиена
      - Хранение логинов и паролей от учетных записей в легкодоступных местах
        - Сохранение паролей в браузерах, клиентах RDP и т.п.
        - Автологон
        - SSO
      - Использование единых паролей для доступа к корпоративным и личным ресурсам
      - Подключение к общедоступным wifi точкам и сетям
  - Используемое оборудование, ПО
    - Специализированные терминальные системы
    - Предустановленные СЗИ
    - BYOD
- Подходы к решению
  - Тчательная настройка пользовательской среды
    - Принцип необходимости и достаточности
      - Корпоративные образы в режиме киоска
      - Тонкие клиенты и ПО для упраления ими
      - Гранулированный доступ к корпоративным данным
    - Биометрия и использование нескольких факторов для аутентификации
    - Предварительная настройка директорий для сохрания данных, политик их очистки
  - Разработка политик хранения данных, внедрение и настройка доверенных файловых хранилищ
    - Приватное облако
    - Выбор коммерческих и публичных информационных ресурсов для хранения данных и работа с ними
    - Разработка корпоративной нормативной документации
      - Категоризация данных
        - Критичность
        - Выбор места хранения
        - Способы и инструменты защиты
      - Правила работы с данными
      - Управление доступом к данным
  - Использование для защиты данных DLP и DCAP решений
    - Какие плюсы?
      - Расширенный аудит
      - Мониторинг потоков данных и своевременное реагирование на проблемы
    - Какие ограничения?
      - Мобильные устройства
      - BYOD
      - Оборудование для удаленного подключения и тонкие клиенты
  - Security Awarness