**Механизм тегирования данных**

**Цели тегирования**:

1. Разграничение уровней доступа.
2. Быстрая идентификация данных для мониторинга и защиты.
3. Поддержка автоматического аудита действий.

**Реализация тегирования**:

1. **Инструменты тегирования**:
   * Метаданные в базе данных (например, колонки с тегами в Postgres).
   * Инструменты DLP (Data Loss Prevention) для автоматической классификации.
   * Платформы Data Governance (Collibra).
2. **Примеры тегов**:
   * PII (личные данные): ФИО, дата рождения, адрес.
   * MEDICAL (медицинские данные): анализы, заключения.
   * FINANCIAL (финансовые данные): счета, чеки.
   * HIGH-RISK (чувствительные данные): данные с высокой степенью риска утечки.
3. **Интеграция тегов**:
   * При добавлении данных в систему автоматически присваивается тег на основе содержания.
   * Теги передаются в систему мониторинга и аудита.

**Инструменты, способы и меры обеспечения конфиденциальности**

1. **Шифрование**:
   * Инструменты: AES-256 для хранения данных, TLS для передачи.
   * Использование аппаратных модулей безопасности (HSM).
2. **Обезличивание**:
   * Инструменты: библиотеки Python (например, FAKER для генерации данных).
   * Методы: удаление персональных идентификаторов (например, ФИО), замена идентификаторов токенами.
3. **Обфускация**:
   * Инструменты: Apache Nifi
   * Применение: в аналитических отчетах, при передаче данных третьим лицам.
4. **Системы управления доступом**:
   * RBAC: разграничение доступа по ролям.
   * ABAC: использование контекстных атрибутов для ограничения доступа.
5. **Мониторинг и аудит**:
   * Системы SIEM для анализа логов.
   * Настройка DLP для предотвращения утечек.
6. **Токенизация**:
   * Инструменты: HashiCorp Vault.
   * Использование токенов вместо реальных данных в API.
7. **Контроль версий и резервное копирование**:
   * Инструменты: Veeam.
   * Периодические резервные копии данных с возможностью восстановления.