Техническое задание по госту ISO шаблон SRS по теме: БАЗА ИНТЕРПОЛА

Шаблон Спецификации Требований к Системе (SRS)

1. Введение

База данных Интерпола — это система, которая собирает, хранит и обрабатывает информацию о преступлениях, разыскиваемых лицах, украденных предметах и других данных, которые могут быть полезны для правоохранительных органов стран-участниц.1.1. Название документа: Спецификация требований к системе для базы данных Интерпола

1.2. Версия: [номер версии]

1.3. Автор: [ФИО или название организации]

2. Общее описание

Содержит информацию, предоставленную странами-членами Интерпола. Проверка по базе Интерпола позволяет правоохранительным органам проверить, есть ли информация о человеке или объекте, связанная с международным розыском, преступлениями, терроризмом, угоном транспортных средств, контрабандой и другими преступлениями.

2.1. Цели системы: Обеспечение эффективного хранения, обработки и поиска информации о разыскиваемых лицах.

3. Функциональные требования

3.1. Регистрация пользователей:

Регистрация пользователей в базе данных Интерпола — это строго контролируемый процесс, поскольку доступ к этой информации имеют только уполномоченные правоохранительные органы. Обычно процесс регистрации включает следующие этапы:

1. **Запрос на доступ**: Правоохранительное учреждение, желающее получить доступ к базе данных Интерпола, должно подать официальный запрос. Это может быть сделано через национальный центральный офис Интерпола (NCB).

2. **Проверка полномочий**: Интерпол проводит проверку, чтобы убедиться, что запрашивающее учреждение имеет законные полномочия и нуждается в доступе к информации для выполнения своих обязанностей.

3. **Обучение и сертификация**: Сотрудники правоохранительных органов, которые будут использовать базу данных, могут проходить обучение по использованию системы и соблюдению протоколов безопасности.

4. **Создание учетной записи**: После одобрения запроса создается учетная запись для соответствующих пользователей. Это может включать назначение уникальных идентификаторов и паролей.

5. **Управление доступом**: Интерпол устанавливает уровни доступа в зависимости от роли пользователя. Некоторые пользователи могут иметь полный доступ к информации, в то время как другие могут иметь ограниченный доступ.

6. **Мониторинг и аудит**: Доступ к базе данных Интерпола подлежит постоянному мониторингу и аудиту, чтобы предотвратить несанкционированный доступ или злоупотребление информацией.

7. **Обновление информации**: Пользователи обязаны поддерживать свои учетные записи актуальными и сообщать о любых изменениях в статусе или полномочиях. Эти меры помогают обеспечить безопасность и конфиденциальность данных, а также гарантировать, что информация используется только в законных целях.

3.2. Управление данными:

Управление данными в базе данных Интерпола осуществляется через ряд строгих процедур и протоколов, чтобы обеспечить безопасность, точность и законность обработки информации. Основные аспекты управления данными в базе Интерпола включают:

1. **Сбор данных**: Данные собираются от стран-членов Интерпола, правоохранительных органов и других уполномоченных организаций. Это может включать информацию о преступниках, розыске, событиях и другие важные данные.

2. **Верификация и валидация**: Все данные проходят процесс проверки на точность и полноту. Это может включать сопоставление с другими источниками информации и подтверждение данных с помощью национальных центральных офисов (NCB).

3. **Классификация и категоризация**: Данные организуются по категориям, таким как тип преступления, географическое положение и другие критерии, что облегчает их поиск и анализ.

4. **Хранение данных**: Данные хранятся в защищенных базах данных с использованием современных технологий шифрования и защиты информации. Это помогает предотвратить несанкционированный доступ.

5. **Доступ к данным**: Доступ к базе данных строго контролируется. Пользователи должны иметь соответствующие полномочия, и доступ предоставляется на основе необходимости. Каждый пользователь имеет уникальный идентификатор и пароль.

6. **Мониторинг и аудит**: Все действия пользователей в системе отслеживаются для обеспечения безопасности и предотвращения злоупотреблений. Регулярные аудиты помогают выявлять и устранять потенциальные уязвимости.

7. **Обновление и удаление данных**: Данные регулярно обновляются для поддержания актуальности. Если информация становится устаревшей или неактуальной, она может быть удалена в соответствии с установленными процедурами.

8. **Соблюдение законодательства**: Интерпол соблюдает международные нормы и стандарты по защите данных, включая GDPR (Общий регламент по защите данных) в Европе, а также другие соответствующие законы в странах-членах.

9. **Обучение пользователей**: Сотрудники, работающие с базой данных, проходят обучение по вопросам безопасности данных и соблюдения протоколов работы с информацией. Эти меры помогают обеспечить эффективное управление данными, защиту конфиденциальности и соблюдение правовых норм в работе Интерпола.

3.3. Поиск данных:

1. **Аутентификация и авторизация**: • **Аутентификация**: Перед тем как получить доступ к базе данных, пользователь должен пройти процедуру аутентификации, которая включает ввод уникального логина и пароля. • **Авторизация**: После успешной аутентификации система проверяет права доступа пользователя. Разные пользователи могут иметь различные уровни доступа в зависимости от их роли (например, офицеры, аналитики, администраторы).

2. **Уровни доступа**: • **Ограниченный доступ**: Некоторые пользователи могут иметь доступ только к определенным категориям данных (например, только к информации о розыске). • **Расширенный доступ**: Пользователи с более высокими привилегиями могут иметь доступ ко всей базе данных или к более чувствительной информации (например, данные о международных преступниках). • **Специальные права**: Некоторые пользователи могут иметь временные права на доступ к определенной информации для выполнения конкретных задач.

3. **Интерфейс поиска**: • Система предоставляет интерфейс для поиска данных, который может варьироваться в зависимости от уровня доступа пользователя. • Пользователи могут использовать различные фильтры и параметры поиска, такие как имя, дата рождения, страна, тип преступления и другие критерии.

4. **Логи и мониторинг**: • Все действия пользователей фиксируются в логах для обеспечения безопасности и возможности последующего аудита. • Администраторы могут отслеживать, какие данные запрашиваются и кем, что помогает предотвратить несанкционированный доступ.

5. **Обучение пользователей**: • Пользователи проходят обучение по вопросам безопасности данных и правильному использованию системы поиска, чтобы минимизировать риск ошибок или злоупотреблений.

6. **Протоколы безопасности**: • При поиске данных применяются протоколы шифрования для защиты передаваемой информации. • Система может включать механизмы обнаружения аномалий для выявления подозрительных действий.

7. **Регулярные обновления и аудит**: • База данных и механизмы поиска регулярно обновляются для улучшения функциональности и безопасности. • Проводятся регулярные аудиты для оценки соблюдения протоколов безопасности и эффективности управления данными. Таким образом, поиск данных в базе Интерпола осуществляется с учетом уровня привилегий пользователей, что обеспечивает безопасность и защиту конфиденциальной информации.

3.4. Отчетность:

Отчетность в базе данных Интерпола включает в себя процессы сбора, обработки и анализа данных, связанных с международной преступностью и правопорядком. Вот как это работает:

**1.** Сбор данных • **Ввод информации**: Члены Интерпола (страны и правоохранительные органы) вводят данные о преступлениях, подозреваемых, арестах и других событиях в базу данных. • **Разнообразие источников**: Данные могут поступать из различных источников, включая национальные базы данных, международные организации и отчеты о преступлениях.

**2.** Стандартизация данных • **Единые форматы**: Для обеспечения совместимости данные стандартизируются по определенным форматам и критериям. Это позволяет различным странам и организациям легко обмениваться информацией. • **Кодирование**: Используются уникальные идентификаторы для каждого объекта (например, для лиц, организаций и преступлений), что упрощает поиск и анализ.

**3.** Обработка данных • **Анализ и фильтрация**: Данные обрабатываются с использованием аналитических инструментов для выявления тенденций, паттернов и аномалий. • **Создание отчетов**: На основе обработанных данных формируются различные типы отчетов (стандартные, специальные, аналитические).

**4.** Генерация отчетов • **Автоматизация**: Многие отчеты генерируются автоматически на регулярной основе, например, ежемесячно или quarterly. • **Настройка отчетов**: Пользователи могут настраивать отчеты в зависимости от своих потребностей, выбирая необходимые параметры и фильтры.

**5.** Доступ к отчетам • **Уровни доступа**: Доступ к отчетам регулируется в зависимости от роли пользователя. Например, администраторы могут видеть все отчеты, в то время как обычные пользователи имеют доступ только к определенным данным. • **Интерфейс пользователя**: Отчеты доступны через специализированные интерфейсы, которые позволяют пользователям легко находить нужную информацию▎

**6.** Использование отчетов • **Оперативная работа**: Отчеты помогают правоохранительным органам принимать оперативные решения, проводить расследования и координировать действия на международном уровне. • **Анализ тенденций**: Аналитические отчеты используются для выявления новых угроз и разработки стратегий борьбы с преступностью.

**7.** Обратная связь и улучшение • **Сбор отзывов**: Пользователи могут предоставлять отзывы о качестве отчетов, что позволяет улучшать процессы сбора и анализа данных. • **Обновление систем**: На основании обратной связи могут проводиться обновления программного обеспечения и методов работы.

**8.** Безопасность и конфиденциальность • **Защита данных**: Все данные защищены с помощью современных технологий шифрования и контроля доступа, чтобы предотвратить несанкционированный доступ. • **Логи действий**: Все операции с отчетами фиксируются в логах для обеспечения возможности аудита и мониторинга безопасности.

4. Нефункциональные требования

4.1. Производительность:

 Минимальные требования для сервера базы данных:

Процессор. 2 ядра, тактовая частота 2,4 ГГц и выше.

Оперативная память. 4 ГБ и выше.

Видеокарта. Видеокарты с поддержкой Shader Model 3.0, например Nvidia GeForce 6600 и

выше, ATI Radeon X1300 и выше, чипсеты Intel G35 (GMA X3500), Intel G4x, Q4x и выше.

Жёсткий диск. Свободный объём от 20 ГБ.

Монитор. Разрешение экрана 1920х1080, диагональ 22 дюйма и выше.

Аппаратные требования рассчитываются индивидуально для каждой прикладной системы на основании результатов нагрузочного тестирования.

Время ответа на запрос не должно превышать 2 секунд.

4.2. Безопасность:

**Обеспечение конфиденциальности и защита информации от несанкционированного доступа.**

**Назначение информации только для использования правоохранительными и судебными органами.**

Также в рамках защиты базы данных Интерпола **данные должны быть точными, актуальными и не избыточными**. Генеральный секретариат устанавливает механизмы и инструменты, чтобы гарантировать соблюдение этого требования.

Кроме того**, данные могут храниться в базах Интерпола только на время, необходимое для достижения цели, для которой они были записаны.** Обычно первоначальный срок хранения не превышает пять лет, если более короткий срок не установлен национальным законом или цель не достигнута.

4.3. Доступность:

База данных Интерпола работает круглосуточно, 24 часа в сутки, 7 дней в неделю. Это необходимо для обеспечения оперативного доступа к информации о разыскиваемых лицах, украденных предметах и других данных, которые могут быть критически важны для правоохранительных органов по всему миру. Системы Интерпола обеспечивают постоянный мониторинг и обновление данных, что позволяет странам-участницам быстро реагировать на угрозы и преступления. Конкретные временные рамки для обновления базы данных Интерпола и исправления ошибок на сайте могут варьироваться в зависимости от различных факторов, но вот примерные ориентиры:

1. **Обновление баз данных**: • **Информация о разыскиваемых лицах**: Обычно обновляется в течение 24-48 часов после получения новых данных от стран-участниц. • **Данные о украденных предметах**: Могут обновляться еженедельно или по мере поступления новой информации, в зависимости от срочности и важности.

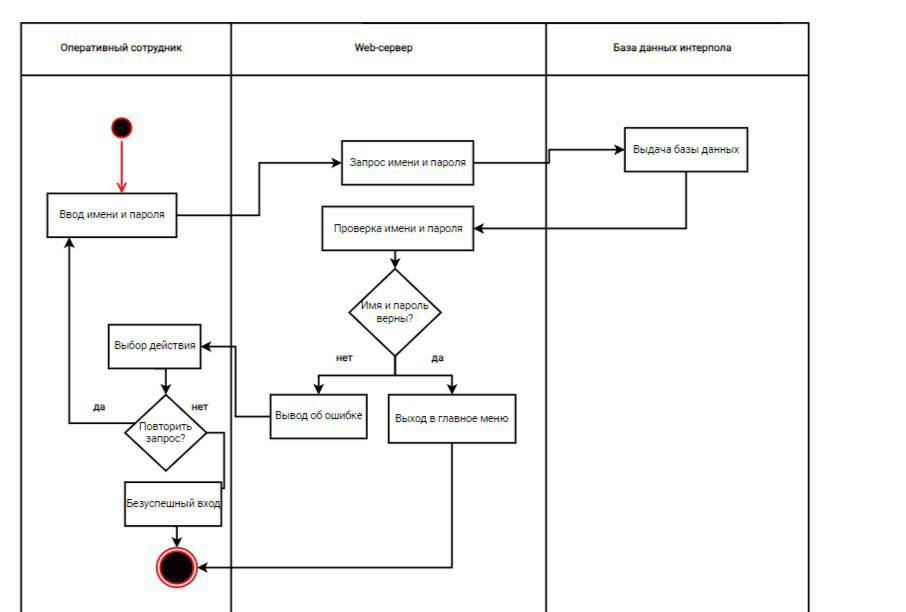
2. **Исправление ошибок на сайте**: • **Незначительные ошибки (например, опечатки)**: Обычно могут быть исправлены в течение нескольких дней до недели. • **Серьезные ошибки (например, неверная информация о разыскиваемом лице)**: Должны быть исправлены как можно скорее, часто в пределах 24-48 часов, чтобы избежать возможных правовых последствий или недоразумений.

Эти временные рамки являются ориентировочными и могут изменяться в зависимости от внутренних процессов Интерпола и объема работы.

5. Приложения

5.1. Диаграммы (ER-диаграммы, диаграммы потоков данных и т.д.).

Диаграмма деятельности для Оперативного сотрудника и администратора:



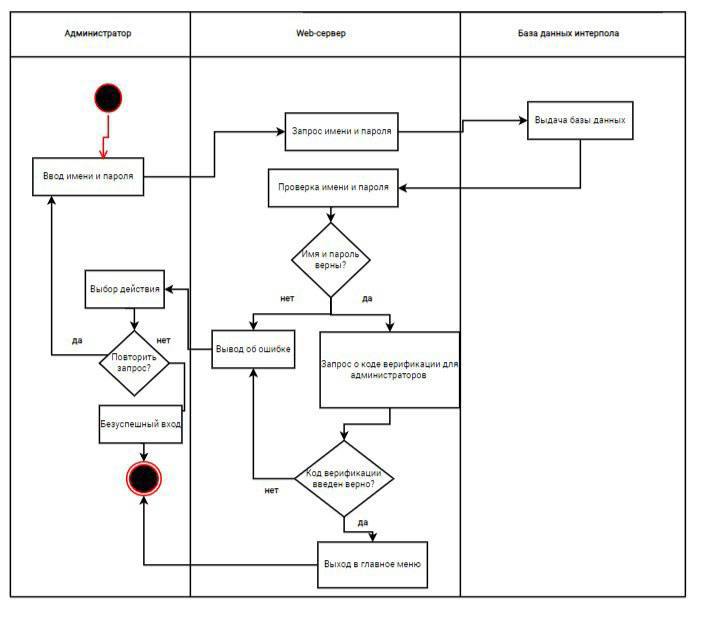


Диаграмма состояния:

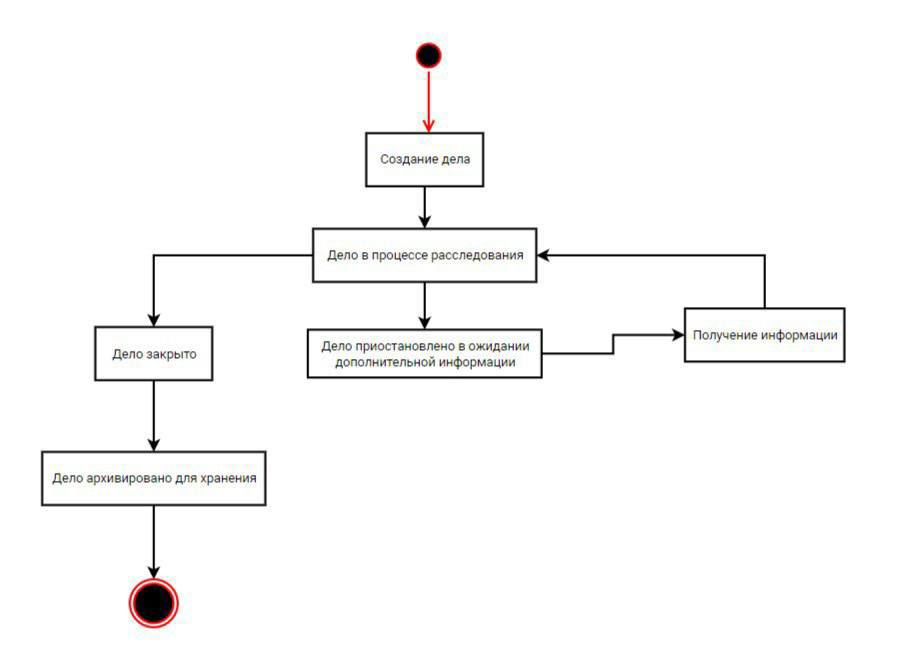


Диаграмма классов:

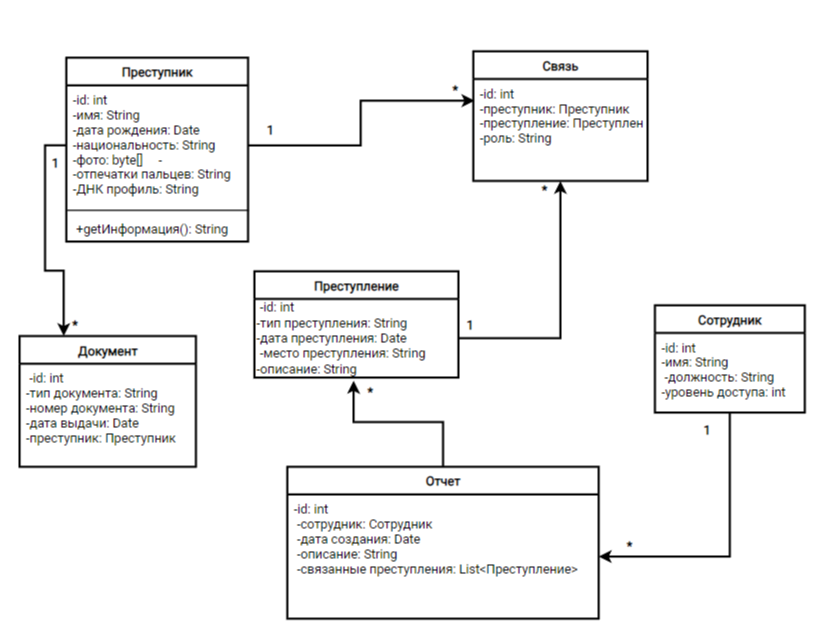


Диаграмма развёртывания:

