**Руководство пользователя и администратора**

1. Введение

Руководство предназначено для пользователей и администраторов подсистемы хранения данных системы распознавания дефектов на текстиле. Оно содержит информацию о функциональности Подсистемы, ее настройке и эксплуатации.

1. Обзор подсистемы

Подсистема предназначена для хранения и управления данными о дефектах ткани, выявленных Системой. Она предоставляет API для доступа к этим данным другим компонентам Системы.

1. Роли пользователей

* Пользователь (Оператор): Имеет доступ к чтению данных о дефектах, добавлению новых дефектов, обновлению информации о существующих дефектах и удалению дефектов.
* Администратор: Имеет полный доступ ко всем функциям Подсистемы, включая управление пользователями, настройку системы, резервное копирование и восстановление данных.

1. Руководство пользователя (Оператора)
   1. Доступ к API:
   * Для доступа к API Подсистемы необходимо использовать HTTP-клиент.
   * Необходимо получить токен аутентификации от администратора.
   1. Добавление нового дефекта:
   * Используйте метод POST/defects.
   * Необходимо предоставить данные о дефекте в формате JSON в теле запроса.
   * В случае успешного добавления, API вернет код 201 (Created) и JSON с данными о созданном дефекте, включая его идентификатор.
   1. Получение информации о дефекте:
   * Используйте метод GET/defects/{defect\_id}, где {defect\_id} - идентификатор дефекта.
   * В случае успешного получения, API вернет код 200 (OK) и JSON с данными о дефекте.
   * В случае, если дефект не найден, API вернет код 404 (Not Found).
   1. Обновление информации о дефекте:
   * Используйте метод PUT/defects/{defect\_id}, где {defect\_id} - идентификатор дефекта.
   * Необходимо предоставить данные о дефекте в формате JSON в теле запроса.
   * В случае успешного обновления, API вернет код 200 (OK) и JSON с обновленными данными о дефекте.
   * В случае, если дефект не найден, API вернет код 404 (Not Found).
   1. Удаление дефекта:
   * Используйте метод DELETE/defects/{defect\_id}, где {defect\_id} - идентификатор дефекта.
   * В случае успешного удаления, API вернет код 204 (No Content).
   * В случае, если дефект не найден, API вернет код 404 (Not Found).
   1. Поиск дефектов:
   * Используйте метод GET/defects.
   * Можно использовать параметры запроса для фильтрации результатов. Например: /defects?type=дыра - поиск дефектов типа "дыра".

* API вернет код 200 (OK) и JSON с массивом дефектов, соответствующих критериям поиска.

1. Руководство администратора
   1. Установка и настройка:
   * Настройка базы данных: Необходимо настроить подключение к базе данных в конфигурационном файле Подсистемы.
   * Настройка API: Необходимо настроить параметры API (порт, хост, параметры безопасности) в конфигурационном файле Подсистемы.
   1. Управление пользователями:
   * Администратор имеет право создавать, удалять и изменять права доступа пользователей.
   * Управление пользователями осуществляется через API или через веб-интерфейс администратора.
   * При создании пользователя необходимо указать его логин, пароль и роль.
   1. Резервное копирование и восстановление данных:
   * Регулярное резервное копирование данных является важной частью администрирования Подсистемы.
   * Необходимо настроить еженедельное автоматическое резервное копирование базы данных.
   1. Мониторинг:

* Администратор должен отслеживать состояние Подсистемы (загрузку сервера, использование дискового пространства, количество ошибок).
* Рекомендуется использовать инструменты мониторинга, такие как Prometheus и Grafana.
  1. Обновление программного обеспечения:
* Необходимо регулярно обновлять программное обеспечение Подсистемы для получения новых функций и исправления ошибок безопасности.
* Перед обновлением необходимо сделать резервную копию данных.

1. Устранение неполадок

* Ошибка подключения к базе данных: Проверьте параметры подключения к базе данных в конфигурационном файле.
* Ошибка аутентификации: Проверьте правильность токена аутентификации. Убедитесь, что токен не истек.
* Ошибка сервера (500): Проверьте логи сервера на наличие ошибок. Обратитесь к разработчикам.
* Некорректные данные: Проверьте формат и правильность передаваемых данных.

1. Безопасность

* Не храните пароли в открытом виде.
* Используйте надежные пароли.
* Регулярно обновляйте программное обеспечение для исправления уязвимостей.
* Ограничьте доступ к Подсистеме только авторизованным пользователям.
* Используйте шифрование для защиты данных при передаче по сети.