Whitepaper

152-ФЗ и on-device ML в ритейле

Архитектура обработки данных Zorky для ИБ-служб, DPO и юристов ритейла

Версия 1.0 · 5 ноября 2026 · zorkypoisk.ru

Документ описывает фактическую архитектуру продукта. Не является юридическим заключением и не заменяет оценку соответствия 152-ФЗ юристом и оператором данных заказчика.

Оглавление

- 1. Для кого этот документ и как его читать
- 2. Что такое on-device ML простыми словами
- 3. Какие данные обрабатывает Zorky: карта потоков
- 4. Что уходит в бэкенд, что нет
- 5. Модель угроз и как мы её снижаем
- 6. 152-ФЗ: что относится к продукту, что — к заказчику
- 7. Какие документы запросить у вендора перед пилотом
- 8. Контакты для ИБ-брифинга

1. Для кого этот документ и как его читать

Документ адресован ИБ-службе, DPO, юристам и архитекторам ритейла, которые валидируют вендора computer vision до пилота. Цель — одинаковое понимание: где выполняется распознавание, какие данные покидают устройство, что можно запросить у вендора.

Как читать: разделы 2–5 — архитектура; раздел 6 — границы ответственности по 152-ФЗ без гарантийных формул; раздел 7 — чеклист документов; раздел 8 — контакт для брифинга.

Сноска 1. Внутренний источник: посадочная https://zorkypoisk.ru/privacy-on-device-ml и продуктовое описание on-device контура Zorky (промты #8–#10).

2. Что такое on-device ML простыми словами

On-device ML означает, что модель и логика распознавания выполняются на смартфоне сотрудника внутри мобильного приложения (МПС). Кадр с камеры не обязан уходить на сервер, чтобы получить результат поиска по коду или этикетке.

Zorky поставляет SDK: общая бизнес-логика на Kotlin Multiplatform, нативные слои Android/iOS для камеры и инференса, callback в UI МПС. Команде заказчика не нужно обучать CV-модель с нуля для типовых сценариев.

Сноска 2. Архитектура SDK: https://zorkypoisk.ru/mps-sdk

3. Какие данные обрабатывает Zorky: карта потоков

Локальный контур: кадр камеры → детекция/OCR этикетки или кода → сопоставление со сценарием → подсветка в UI. Все эти шаги выполняются на устройстве.

Целевой сценарий — чтение кодов и этикеток для операционного поиска, а не идентификация человека по лицу. Юридическая квалификация отдельных полей зависит от конфигурации заказчика и применимого права.

Сноска 3. Операционный офлайн-сценарий: https://zorkypoisk.ru/offline-warehouse-vision

4. Что уходит в бэкенд, что нет

Таблица отражает целевую архитектуру. Конфигурация конкретной сети может отличаться и фиксируется на ИБ-брифинге.

Данные | В бэкенд? | Комментарий
Кадры с камеры | Нет | Обрабатываются на устройстве
Распознанный артикул/код | Только агрегированно | В рамках метрик сценария
Идентификатор сотрудника | По конфигурации заказчика | Может быть псевдонимизирован
Метрики поиска | Да | Для админки и аналитики
ФИО, телефон | Нет | Вне скоупа продукта

Сноска 4. Таблица потоков согласована с публичным описанием на /privacy-on-device-ml. Поля логов и TTL — уточняются на ИБ-брифинге.

5. Модель угроз и как мы её снижаем

- Утечка кадров из облака — снижается тем, что кадры не выгружаются как изображения в облако Zorky.
- Перехват трафика распознавания — снижается: шаг инференса не требует сети.
- Подмена модели на устройстве — целостность поставки и обновлений уточняется на брифинге.
- Утечка через логи — политика логов уточняется на брифинге и в ответах на опросный лист.

Это не заявление об абсолютной защищённости. Меры снижают риск; ответственность за конфигурацию и эксплуатацию остаётся за заказчиком.

Сноска 5. Формулировки модели угроз — по публичной посадочной приватности Zorky; без ссылок на неподтверждённые сертификаты регулятора.

6. 152-ФЗ: что относится к продукту, что — к заказчику

Оценка соответствия 152-ФЗ — зона юриста и оператора данных заказчика. Продукт описывает архитектуру минимизации данных, покидающих устройство.

- Продукт: on-device инференс; прозрачный data flow; готовность ответить на опросный лист ИБ.
- Заказчик: цели обработки, правовые основания, внутренние политики, решение включать ли ID сотрудника.
- Сделка: NDA/DPA по шаблону заказчика или согласованное приложение.

Мы не публикуем гарантийные формулы соответствия на лендинге. Данный whitepaper также не является юридическим заключением.

Сноска 6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» — публичный источник; применение к конкретной конфигурации — к юристу заказчика.

7. Какие документы запросить у вендора перед пилотом

- Архитектурная схема on-device обработки
- Описание потоков данных (data flow)
- Ответы на опросный лист ИБ (формат согласуем)
- NDA / DPA по шаблону заказчика
- Контакт технического ответственного

Рекомендуемый формат старта — ИБ-брифинг 45–60 минут с фиксацией письменных ответов.

Сноска 7. Чеклист документов — по посадочной https://zorkypoisk.ru/privacy-on-device-ml

8. Контакты для ИБ-брифинга

Email: info@softverno.ru

Страница для ИБ: https://zorkypoisk.ru/privacy-on-device-ml

HTML-версия этого документа: https://zorkypoisk.ru/docs/whitepaper-152fz-on-device-ml

Заявка на брифинг — через форму на сайте (событие заявки demo_request).

Версия и дисклеймер

Версия 1.0 от 5 ноября 2026. Издатель: Zorky / softverno. Документ может обновляться; актуальная HTML-версия публикуется на zorkypoisk.ru. Не является юридическим заключением, офертой или гарантией соответствия требованиям законодательства.