

PII Firewall

Обезличивание рабочих документов перед отправкой во внешнюю языковую модель.

Период: 08/2026 – наст. время

Роль: автор продукта (архитектура, детекция, шифрование, интерфейс, проверки безопасности в CI)

Исходный код закрыт

ЗАДАЧА

Запрет на внешние языковые модели обычно держится до первой срочной задачи. Потом договор с персональными данными попадает к третьей стороне. Готовые PII-детекторы рассчитаны на западные форматы и не отличают ИНН от номера договора такой же длины.

РЕШЕНИЕ

- На входе файлы PDF, DOCX и XLSX. На выходе обезличенный текст и зашифрованная карта замен, ответ модели возвращается с исходными значениями.
- Четыре слоя детекции: структурные правила с контрольными суммами идентификаторов, NER-модель GLiNER на видеокarte, словарь с морфологическим ключом и слой учётных данных. Найденные учётные данные блокируют документ целиком.
- У зоны обезличивания нет маршрута ни в интернет, ни к модели. Поэтому ошибка в её коде не может привести к исходящему запросу.
- Карта замен расшифровывается только внутри контура и только для пользователя, который загрузил документ.
- Документы с номером медицинского полиса относятся к данным о здоровье и по умолчанию отправляются только в локальную модель.

РЕЗУЛЬТАТЫ

- Синтетический эталон, 40 документов и 322 вхождения: полнота 100%, точность 100%.
- Восстановление побайтно совпало с оригиналом в 20 случаях из 20.
- Следующий этап проверки: реальные документы и корпуса публичных актов.

ТЕХНОЛОГИИ

Python · GLiNER · OCR · Envelope encryption · Keycloak SSO · Docker · GitLab CI