Распознавание лиц в видеонаблюдении - справка на одной странице

Как работает распознавание, насколько оно точно вне лаборатории, как событие лица попадает в VMS и где проходит граница закона. Представительные цифры 2025-2026 - всё зависит от качества изображения, ракурса, света и людей в кадре.

A. Детекция - это не распознавание

- ДЕТЕКЦИЯ лица лишь находит, что лицо есть (рамка) - анонимно, легко, работает на камере, почти без веса приватности.
- РАСПОЗНАВАНИЕ измеряет лицо в шаблон и решает, ЧЬЁ это лицо - именно этот шаг является биометрией и юридическим барьером.
- Тест: пытается ли система различать людей и присваивать им имя или устойчивую личность? Если да - действует юр. барьер.
- Вендоры размывают разницу. 'AI по лицам' может означать только детекцию (безвредно) или полное распознавание (жёстко регулируется). Всегда уточняйте.

B. Конвейер из четырёх шагов

- 1 Детекция: найти и вырезать лицо. 2 Выравнивание: по точкам (глаза, нос, рот) привести лицо к стандартному ракурсу.
- 3 Эмбеддинг: нейросеть превращает лицо в шаблон - вектор ~512 чисел (напр. ArcFace). Шаблон - это числа, а НЕ сохранённое фото.
- 4 Сверка: сравнить шаблоны по сходству (cosine) против ПОРОГА. Превысил = совпадение. Порог - регулятор; идеального значения для всех нет.
- Верификация 1:1 (сотрудничающий; СКУД, разблокировка) точна. Идентификация 1:N (список наблюдения; наблюдение) - трудный случай.

C. Точность - диапазон, и вне лаборатории она рушится

- Кооперативные портреты NIST (1:1): лучшие алгоритмы выше ~99% (ошибка < 0,1% на визовом качестве). Это ЛАБОРАТОРНАЯ цифра.
- Реальное CCTV (1:N): ТОТ ЖЕ алгоритм часто падает до ~65-85% - ракурс, движение, низкое разрешение, дистанция. Никогда не 100%.
- Ложные срабатывания 1:N растут с галереей: 1 000 000 проверок x 0,1% = ~1000 ошибок в день.
- Ошибок больше у женщин, пожилых, детей и части демографических групп (NIST FRVT Part 3). Совпадение - это ЗАЦЕПКА, а не доказательство.

D. Как событие лица попадает в VMS - и где это работает

- ONVIF Profile M стандартизирует канал события/метаданных лица в VMS (по потоку, через ONVIF event service или MQTT).
- ONVIF стандартизирует СОБЫТИЕ, а не точность и не алгоритм - модель, галерея и порог живут в SDK вендора. Совместимость - базовый уровень.
- Детекция работает на КРАЮ (NPU камеры). Распознавание - на СЕРВЕРЕ/В ОБЛАКЕ: ему нужна галерея шаблонов в одном месте.
- Эта центральная галерея - концентрированное хранилище биометрии, самый регулируемый актив. Держите её минимальной и под контролем доступа.

E. Юридический барьер: шаблон лица - это биометрия

- GDPR ст. 9: биометрия для однозначного опознания - спец-категория, запрещена без узкого исключения; DPIA по ст. 35 (EDPB Guidelines 3/2019).
- EU AI Act ст. 5: real-time опознание в публичных местах - запрещённая практика для большинства целей (в силе с 2 фев 2025); прочее биом. ID - высокий риск.
- США, Illinois BIPA (740 ILCS 14): сперва письменное согласие; частный иск; штрафы $1000/$5000 (Facebook урегулировал на $650 млн).
- США, Texas CUBI: иск AG; $1,4 млрд с Meta (2024). Лоскутное право - действует строжайшее правило. Инженерное руководство, не юр. совет.

Чистое правило: распознавание лица - это юридический барьер, через который проходят до того, как выпускать фичу: подтвердите законное основание и режим согласия, проведите DPIA, держите галерею минимальной и под контролем доступа, задайте максимальный по закону срок хранения, считайте каждое совпадение проверяемой зацепкой и привлеките юриста по вашей юрисдикции. МОДЕЛЬ распознавания (архитектуры эмбеддингов, обучение ArcFace) разрабатывается в разделе AI for Video Engineering; здесь - ПРИМЕНЕНИЕ в наблюдении. Источники: ONVIF Profile M; GDPR Per. (ЕС) 2016/679 ст. 4(14), 9, 35; EDPB Guidelines 3/2019; EU AI Act Per. (ЕС) 2024/1689 ст. 5; Illinois BIPA 740 ILCS 14; Texas CUBI / $1,4 млрд Meta; NIST FRVT Part 3 (NISTIR 8280) и FRTE; ArcFace (arXiv 1801.07698); ACLU Williams v. City of Detroit.