

Чек-лист архитектуры и управления городским видеонаблюдением

Спланируйте городское или публичное видеонаблюдение по двум определяющим нагрузкам — масштабу и весу приватности — до закупки оборудования. Дополнение к статье; используйте вместе с моделью стоимости видеонаблюдения.

1 · Две нагрузки — проектируйте под обе сразу

Город определяют экстремальный масштаб (тысячи камер, много вендоров, районов и ведомств) И самый тяжёлый вес приватности в видеонаблюдении: он смотрит на публику в местах, которых не избежать. Дизайн, отвечающий лишь на одну из двух, проваливается. Планируйте архитектуру и комплаенс вместе, с первой схемы.

2 · Федерация — пишите локально, поток по запросу

Не централизуйте. Стройте по одной системе на район, которая пишет свои камеры локально, плюс тонкий слой, дающий центру искать по всему городу и открывать любую камеру по запросу. Централизация 5000 камер потребовала бы ~10 Gbps постоянного канала и сделала бы центр единой точкой отказа; федерация несёт лишь метаданные и потоки, что открыл оператор. Разнородный парк держите на ONVIF (Profile S/G/T/M), а требования задавайте по IEC 62676.

3 · Расчёт хранения и канала (покажите математику)

Рычаг	Результат
1 Mbps постоянно	= 10,8 ГБ / камера / сутки
5000 камер x 2 Mbps	= 108 ТБ / сутки
x 30 суток хранения	= 3,2 ПБ полезных (~4,9 ПБ сырых с RAID + запас)
Канал: центр vs федерация	~10 Gbps постоянно vs ~200 Mbps по запросу

Срок хранения, режим записи и уровни хранения — это бюджет, а не характеристики камеры.

4 · Барьер биометрии / закона — отметьте до любого сличения лиц

☐

Распознавание лиц публики в реальном времени ВЫКЛ по умолчанию — это барьер закона, не переключатель.

☐

EU AI Act ст. 5(1)(h): биометрическая идентификация в реальном времени в публичных местах запрещена для полиции (в силе с 2 фев 2025), кроме узких исключений с санкцией суда.

☐

Шаблон лица — особые данные GDPR ст. 9; номер ANPR / LPR — персональные данные, но не биометрия.

☐

Сверьте юрисдикцию: Великобритания (дело Bridges) и запреты городов США (напр., Сан-Франциско) сильно различаются.

☐

Любая биометрия: предварительная санкция, оценка влияния на права / данные и журнал.

5 · Управление privacy-by-design — встраивайте, не навешивайте

☐

Задokumentированы основание и цель для каждой камеры и аналитики; камеры направлены не шире нужного.

☐

DPIA выполнен до запуска (GDPR ст. 35) — это норма для масштабного наблюдения за публичным местом.

☐

Маскирование зон, за которыми системе незачем смотреть (окна, интерьеры, участок соседа).

☐

Срок хранения минимально нужный; удаление по расписанию с журналом (GDPR ст. 5(1)(e)).

☐

Ролевой доступ по ведомствам, с полным журналом всех просмотров, поисков и выгрузок.

Инженерное руководство, не юридическая консультация. Барьер закона называет EU AI Act (Reg. (EU) 2024/1689) ст. 5, GDPR ст. 9 / ст. 35 / ст. 5(1)(e), Guidelines EDPB 3/2019 и британское дело Bridges; сверьтесь с квалифицированным юристом до запуска любой аналитики опознания.