

Чек-лист интеграции умного здания и кампуса

Спланируйте видеонаблюдение умного здания или кампуса по его интеграции — какие подсистемы доходят до оператора, какой стандарт несёт каждую связь, как федерируется кампус и где проходит граница приватности — до закупки оборудования. Дополнение к статье; используйте с моделью стоимости.

1 • Правило: здание — одна система, камера — лишь часть

Ценность не в камерах, а в том, разговаривают ли они с дверями, тревогами и инженерией здания. Тест интеграции: событие взлома двери само вызывает нужную камеру на один экран и предлагает блокировку в один клик - а не заставляет оператора искать среди 400 камер. Решите заранее: одна единая платформа (видео + СКУД + охрана в одном продукте) или отдельные лучшие-в-классе системы, связанные через стандарты и SDK; работают оба, но именно связи и есть проект.

2 • Задайте стандарт на каждую связь

Связь	Какой стандарт указать	Примечание
Видео	ONVIF Profile S / T / G	Глубокие функции всё равно требуют SDK
Конфиг СКУД	ONVIF Profile A	Идентификаторы, расписания, правила
События двери	ONVIF Profile C	Открыта / взлом / удержание; контроль
Связь считыв.	OSDP + Secure Channel	IEC 60839-11-5; вместо Wiegand
Метаданные	ONVIF Profile M	События аналитики; качество разное
Инженерия	BACnet (ISO 16484-5)	Связь с HVAC / свет / лифты / пожар

3 • Кампус, мультиарендность и парк — до запуска

- ☐ Федерация настроена: каждое здание пишет локально и считает на краю; поток по сети — только по запросу (не централизуйте все потоки).
- ☐ Разделы по арендаторам / отделам заданы и закреплены ролевым доступом (RBAC) в модели прав и журнале аудита — а не просто скрыты в интерфейсе.
- ☐ У общих зон (холлы, парковки, периметр) есть явный владелец и центральная межраздельная роль.
- ☐ Управление парком спланировано как система: ввод, прошивки, ротация сертификатов, пароли и мониторинг состояния каждого устройства.
- ☐ Аналитика занятости / использования считает анонимно (счёт, не личность); где нужна только загрузка — лучше некамерные датчики.

4 • Кибербезопасность и барьер приватности — до запуска

- ☐ Камеры, контроллеры и инженерия — в изолированных сегментах сети (VLAN), отделённых от корпоративной сети и интернета.
- ☐ Пароли по умолчанию сменены, сертификаты ротированы, прошивки актуальны по всему парку; OSDP Secure Channel вместо Wiegand.
- ☐ Проверка цепочки поставок (US NDAA ст. 889 / FAR 52.204-25 — список вендоров там, где федеральные деньги, контракты или гранты).
- ☐ Основание мониторинга персонала задокументировано (GDPR ст. 6(1)(f) + необходимость / соразмерность; ст. 88; сотрудники уведомлены где нужно).
- ☐ Камеры вне приватных зон; чёткие таблички / уведомление; срок хранения минимальный (GDPR ст. 5(1)(e)); DPIA при систематическом масштабе (ст. 35).
- ☐ Оpozнание по лицу / отпечатку на двери или камере — за осознанной юр. проверкой: GDPR ст. 9 / Illinois BIPA, не по умолчанию.

Инженерное руководство, не юридическая консультация. Барьер приватности называет GDPR ст. 6(1)(f) / 9 / 35 / 88 / 5(1)(e), Guidelines EDPB 3/2019 и Illinois BIPA (740 ILCS 14) как управляющую рамку; сверьтесь с квалифицированным юристом до запуска любой аналитики персонала или биометрии.