Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

IP-видеонаблюдение в офисе: как мы строим систему под ключ

Типовая схема: камеры 4 Мп, аппаратный NVR, PoE-бюджет, VLAN-изоляция и доступ по WireGuard

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Заказчику нужна доказательная видеозапись инцидентов, а не «камеры для галочки»: архив не должен теряться, камеры — висеть в одной сети с 1С и рабочими станциями, а руководитель должен видеть объект с телефона без проброса портов. Мы собираем систему на Hikvision + выделенный VLAN + WireGuard: иначе запись обрывается в момент кражи, а камера с уязвимой прошивкой становится точкой входа в ЛВС.

Почему это важно бизнесу

- Потерянный архив в день инцидента — недоказуемая кража и спор со страховой: запись должна идти непрерывно и мониториться
- Камера в общей ЛВС — плацдарм атаки: у IP-камер регулярно выходят критические CVE с удалённым выполнением кода
- NVR, проброшенный в интернет, попадает в сканеры ботнетов: риск утечки видеоархива с персональными данными — это уже зона 152-ФЗ
- Desktop-диски не переживают круглосуточную запись: скрытая замена дисков каждые 6–10 месяцев и дыры в архиве

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

4 Мп

рабочее разрешение офисной камеры: 2688×1520, WDR 120 дБ — лица и детали без переплаты за 4K

Hikvision DS-2CD2143G2-I(S)

160 Мбит/с

входящая полоса NVR DS-7616NI-K2/16P — сверяем сумму битрейтов всех камер с запасом на события

по докам Hikvision

450 Вт

гарантированный PoE-бюджет CRS328-24P-4S+RM: 3×150 Вт на каждые 8 портов, до 30 Вт на порт

по докам MikroTik

180 ТБ/год

норматив нагрузки surveillance-дисков WD Purple (AllFrame) и SkyHawk (ImagePerfect)

спецификации WD / Seagate

≈50%

средний битрейт при H.265+ держится около половины max bitrate — так считаем глубину архива

Hikvision H.265+ White Paper

51820/UDP

единственный порт наружу — WireGuard для удалённого просмотра; NVR в интернет не публикуем

наш стандарт / wireguard.com

РЕАЛИЗАЦИЯ 1 ИЗ 3

Сегментация: камеры в выделенном VLAN 30

Что настраиваем

Коммутатор MikroTik CRS328-24P-4S+RM (RouterOS), 16 камер, ядро офисной ЛВС

Как мы это делаем

1. Создаём vlan30-cam на bridge, подсеть 192.168.30.0/24; камерам — фиксированные DHCP-lease по MAC-адресам
2. Firewall forward: accept только cam→NVR по TCP 554 (RTSP) и 8000 (SDK Hikvision), затем drop — камеры не видят ни ЛВС, ни интернет
3. PoE-бюджет: 12 внутренних камер ×6,5 Вт + 4 уличных ×12 Вт = 126 Вт, +30% запас ≈ 164 Вт при гарантированных 450 Вт (3×150 Вт на 8 портов)
4. На портах камер включаем port isolation; зависшую камеру лечим перезапуском PoE-порта (poe-out off/auto-on) удалённо

РЕЗУЛЬТАТ

Скомпрометированная камера не даёт бокового перемещения: нет маршрута ни к рабочим станциям с 1С, ни в интернет; зависшие камеры перезапускаем питанием порта без выезда на объект

КЛЮЧЕВОЙ НЮАНС

PoE-бюджет считаем по максимуму из датащита (ночью с ИК-подсветкой), а не по среднему: 802.3af даёт 15,4 Вт на порт, уличным варифокалам нужен 802.3at до 30 Вт

Запись: NVR Hikvision и расчёт архива

Что настраиваем

NVR DS-7616NI-K2/16P (16 каналов, 16 PoE, 2×SATA) + камеры DS-2CD2143G2-I(S) 4 Мп

Как мы это делаем

1. Кодек H.265+: main stream 2688×1520@20 к/с, max bitrate 4096 Кбит/с — по White Paper средний битрейт держится около половины максимума
2. Расчёт архива: средний битрейт 2 Мбит/с (половина max), 16 камер ≈ 346 ГБ/сутки; 30 дней ≈ 10,4 ТБ, +25% на пиковые сцены ≈ 13 ТБ — ставим 2×10 ТБ WD Purple
3. Сверяем полосу: пик 16×4 Мбит/с = 64 Мбит/с при 160 Мбит/с входящих у NVR — остаётся запас на вторые потоки и события
4. Двухпоточная схема: непрерывно пишем sub-stream, по детекции AcuSense (человек/транспорт) — main stream: 90 дней событийного архива без роста дисков
5. Активация NVR: стойкий пароль, отключаем UPnP и P2P Hik-Connect, время по NTP; включаем алерты «потеря видео» и «ошибка диска»

РЕЗУЛЬТАТ

30 дней непрерывного архива плюс 90 дней по событиям на дисках с нормативом 180 ТБ/год; NVR сам сигнализирует о потере сигнала камеры и SMART-ошибках диска

КЛЮЧЕВОЙ НЮАНС

Диски только surveillance-серий: WD Purple (AllFrame) или SkyHawk (ImagePerfect) держат 180 ТБ/год; desktop-серии не рассчитаны на 24/7-поток и умирают в NVR за 6–10 месяцев

РЕАЛИЗАЦИЯ 3 ИЗ 3

Доступ и контроль: WireGuard вместо облаков

Что настраиваем

Шлюз офиса (MikroTik/Linux), смартфоны руководителя и охраны, наш Zabbix-мониторинг

Как мы это делаем

1. Поднимаем WireGuard на шлюзе: интерфейс wg0, порт 51820/UDP; каждому устройству — свой ключ, /32-адрес и AllowedIPs только до подсети NVR
2. Конфиг раздаём QR-кодом в бесплатное приложение WireGuard; NVR открывается в iVMS-4200/мобильном клиенте по локальному IP через туннель
3. Порты NVR (80/554/8000) наружу не публикуем вообще — доступ существует только внутри туннеля
4. Каждую камеру ставим на ICMP+RTSP-мониторинг: зависание или потеря потока — алерт в Telegram дежурному инженеру

РЕЗУЛЬТАТ

Видео не покидает периметр: без облачных подписок и открытых портов руководитель видит живое видео и архив с телефона; о зависшей камере узнаём мы по алерту, а не клиент в день инцидента

КЛЮЧЕВОЙ НЮАНС

Ключ — на устройство, не на компанию: отзыв доступа уволенного сотрудника = удаление одного peer за минуту, без перевыпуска общих конфигов

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ Камеры в общей сети с рабочими станциями

У IP-камер регулярно выходят критические CVE. Выносим в отдельный VLAN: firewall разрешает только cam→NVR (TCP 554/8000), интернет камерам закрыт.

✕ Desktop-диски в NVR

WD Blue/Barracuda не рассчитаны на 24/7-запись и умирают за 6–10 месяцев. Ставим WD Purple/SkyHawk: норматив 180 ТБ/год, оптимизация ATA-streaming.

✕ PoE-бюджет посчитан по среднему

Ночью с ИК-подсветкой камера потребляет максимум по датащиту. Считаем по max +30% запаса; уличным варифокалам нужен 802.3at, а не 802.3af.

✕ Проброс портов NVR в интернет

Открытые 80/554/8000 быстро находят сканеры ботнетов, а утечка видеоархива с персональными данными — риск по 152-ФЗ. Доступ только через WireGuard (51820/UDP), наружу портов нет.

✕ Дефолтные пароли и включённый UPnP

При активации задаём стойкие пароли камерам и NVR, отключаем UPnP и P2P-облако, прошивки обновляем с официального портала в рамках абонентки.

✕ 4K «на всякий случай»

8 Мп на 16 камерах удваивает битрейт и архив и упирается в 160 Мбит/с входящих NVR. Для офиса хватает 4 Мп; 4K — точечно: номера машин, дальние планы.

✕ Архив не посчитан — кольцо в 5 дней

Диски берут «какие были», запись затирается раньше, чем инцидент обнаружен. Считаем: средний битрейт × камеры × 86 400 с × 30 дней +25% запаса.

✕ Камеры против света и выше 3 метров

Засветка объектива и съёмка «макушек» обесценивают архив. Высота 2,5–3 м, две камеры под 90° на коридор, WDR 120 дБ на входных группах.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Отдельный VLAN для камер, интернет им закрыт, firewall только cam→NVR
- Аппаратный NVR с PoE и диски WD Purple/SkyHawk, архив 30 дней
- Смена дефолтных паролей, отключение UPnP/P2P, время по NTP

НОРМАЛЬНО

- Камеры 4 Мп с WDR 120 дБ и H.265+; запись: непрерывно + события
- Удалённый доступ только через WireGuard, наружу не открыт ни один порт
- Мониторинг каждой камеры (ICMP+RTSP) с алертами в Telegram
- PoE-коммутатор с запасом бюджета 30% и port isolation

ХОРОШО

- Детекция человек/транспорт (AcuSense) вместо простого motion — меньше ложных тревог
- RAID из surveillance-дисков + копия событийного архива за периметр
- ИБП на NVR и PoE-коммутатор: запись живёт при отключении питания
- Абонентка: прошивки, контроль качества записи, замена дисков по SMART

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Камеры вынесены в отдельный VLAN и не имеют доступа в интернет?
- [ ] С NVR снят проброс портов, удалённый доступ только через VPN?
- [ ] Диски в NVR — surveillance-серии, SMART контролируется?
- [ ] Архив реально хранится 30 дней — проверяли запись на самой дальней дате?
- [ ] PoE-бюджет коммутатора посчитан по максимуму потребления с ИК-подсветкой?
- [ ] Дефолтные пароли камер и NVR сменены, UPnP и P2P-облако отключены?
- [ ] Есть мониторинг: о зависшей камере узнаете раньше, чем понадобится запись?
- [ ] Время камер и NVR синхронизировано по NTP — записи пригодны как доказательство?
- [ ] Сотрудники уведомлены под подпись, таблички «Ведётся видеонаблюдение» установлены (152-ФЗ)?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Проектируем и монтируем IP-видеонаблюдение под ключ: камеры, NVR, PoE, VLAN — 8–12 рабочих дней
- Изолируем существующие камеры в VLAN и закрываем проброшенные порты без замены оборудования
- Настраиваем WireGuard-доступ с телефона руководителя — без облаков и подписок
- Берём систему на абонентское обслуживание: мониторинг камер, прошивки, замена дисков
- Оформляем правовую часть: приказ, уведомление сотрудников, таблички по 152-ФЗ

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 DS-2CD2143G2-I(S) Datasheet — 4 MP AcuSense Fixed Dome (hikvision.com — V5.5.113 (2023))

02 DS-7616NI-K2/16P NVR Datasheet (hikvision.com — V4.71.410 (2022))

03 H.265+ Encoding Technology White Paper (hikvision.com — 2016)

04 CRS328-24P-4S+RM Product Specifications (mikrotik.com — 2026)

05 RouterOS Docs: PoE-out, Bridge VLAN Filtering (help.mikrotik.com — RouterOS 7)

06 WD Purple Surveillance HDD Data Sheet (AllFrame) (westerndigital.com — 2023)

07 SkyHawk 3.5 HDD Datasheet (ImagePerfect) (seagate.com — 2022)

08 WireGuard Quick Start / Protocol (wireguard.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.