

Интеллектуальная система видеонаблюдения Insentry

Эксплуатационная документация

Руководство администратора

Оглавление

• О системе Insentry	6
• Системные требования	6
• Установка и обновление ПО Insentry	7
• Установка ПО Insentry	7
• Установка ПО Insentry на Windows	7
• Установка ПО Insentry на Linux	10
• Установка видеонаблюдения Insentry на CentOS Linux с помощью Docker	10
• Установка видеонаблюдения Insentry на Ubuntu Linux с помощью Docker	11
• Установка видеонаблюдения Insentry на Raspberry Pi 4B с помощью Docker	14
• Установка видеоаналитики на Ubuntu Linux	17
• Установка видеоаналитики Insentry на Raspberry Pi 4B	18
• Установка модуля Get для интеграции с внешними системами	20
• Обновление ПО Insentry	20
• Переустановка ПО Insentry	23
• Бэкап базы данных, лицензий и настроек	25
• Импорт настроек, лицензий и базы данных	26
• Удаление ПО Insentry	27
• Администрирование Insentry	28
• Управление устройствами	29
• Управление камерами	29
• Подключение камер к Insentry	29
• Подключение камер автоматически и вручную	30
• Импорт камер из файла конфигурации	33
• Подключение камер с видеорегистратора	38
• Отключение камер	40
• Просмотр списка и статуса работы камер	40
• Настройка камер	44
• Название и описание камеры	46
• Вендор и модель камеры	46
• Параметры подключения	47
• Расположение камеры	49
• Координаты камеры	50
• Настройка видеопотоков	52
• Настройка безопасности камеры. Права доступа	55
• Присвоение камере тегов	56
• Настройка записи в архив	57
• Связанные объекты	59
• Настройка видеоаналитики	60
• Добавление нового детектора	61
• Просмотр статуса работы детекторов	61
• Настройка детекторов	62
• Разметка видеоаналитики	63
• Детектор огня	65
• Вмешательство в работу камеры	67
• Детектор оставленных предметов	70
• Оповещение о движении в кадре	72
• Встроенная аналитика камеры	75
• ONVIF: вмешательство в работу камеры	75

• Температура людей в кадре (интеграция с тепловизором Dahua)	77
• ONVIF: движение в кадре	77
• Аналитика лиц и поведения людей	79
• Движение людей в запрещённом направлении	79
• Детектор людей в запрещённой зоне	80
• Детектор очередей	82
• Детектор толпы	85
• Подсчёт людей	87
• Детектор касок	90
• Распознавание лиц	91
• Детектор падения человека	93
• Пол, возраст, эмоции	95
• Детектор пересечения линии	96
• Аналитика транспорта	98
• Детектор гос. номеров машин	98
• Рекомендуемые разрешения видеопотоков для видеоаналитики	100
• Просмотр списка детекторов и нейросерверов	100
• Интеграции с внешними системами	103
• Подключение новых интеграций	103
• Список интегрированных систем	104
• Реестр устройств	106
• Зоны	108
• Карты	109
• Добавление новой карты	110
• Слои	111
• Добавление источника карт или схем	112
• Строения	112
• Объекты	115
• Справочники	117
• Email уведомления	117
• Расписания	118
• Создание расписания	118
• Просмотр списка расписаний	119
• Редактирование параметров расписания	120
• Настройка интервалов	122
• Удаление расписания	123
• Транспорт	124
• Добавление транспортного средства	124
• Список номеров транспортных средств	124
• События с транспортным средством	125
• Люди	126
• Добавление новой персоны	126
• Список персон	127
• События с персоной	127
• Справочник тегов и расположений	128
• Пользователи	128
• Создание учётной записи	129
• Дублирование учётной записи	130
• Настройки учётной записи	130
• Настройка прав доступа пользователя	132

• Удаление учётной записи	133
• Аудит действий пользователя	133
• Подключение Watch к каталогу LDAP (включение учетных записей Active Directory)	135
• Подключения	136
• Настройка интеграции с ЕЦХД	137
• Настройка интеграции с Telegram ботом	140
• ГИС «Сфера»	142
• Настройки системы	143
• Диагностика на основе лог-файлов	143
• Система серверов	144
• Модули	149
• Настройка модуля Кеер и параметров хранения архива	150
• Добавление каталога	151
• Редактирование каталога	152
• Редактирование названия хранилища	153
• Удаление каталога из хранилища	153
• Изменение лимита записи	154
• Настройка количества камер для записи архива	154
• Репликация архива. Иерархия модулей Insentry	155
• Перенос архива в другую папку или на другой носитель	157
• Настройка модуля Spot	159
• Адрес для внешних подключений	160
• Импорт и экспорт камер	161
• Работа с лицензиями	166
• Активация лицензии	167
• Расширение лицензии	168
• Удаление лицензии	169
• Перевыпуск ключа	170
• Передача данных в облако Insentry Cloud	170
• Прочие настройки	171
• Доступ к локальному серверу Insentry из WAN сети (проброс портов)	171
• Настройка HTTPS соединения	172
• Воспроизведение потока на сайте через NPM плеер	173
• Получение событий видеоаналитики	176
• Решение проблем	179
• Система не обнаруживает камеру	179
• Не записывается архив	181
• Видеопоток не воспроизводится	181
• Видеопоток работает нестабильно	182
• Insentry.Кеер не видит сетевое хранилище или не хватает прав для его использования	185
• Не включается детектор (ползунок нельзя переключить)	186
• Не запускается клиент Insentry после переустановки модуля Insentry Watch	186
• Восстановление базы данных из резервной копии	187
• Insentry.Cloud	188
• Начало работы в Insentry.Cloud	188
• Подключение камер к Insentry.Cloud	189
• Подключение камер к Insentry.Cloud через роутер	190
• Подключение через роутер Keenetic (Zyxel)	190

• Подключение через роутер MikroTik	200
• Подключение камер к Insentry.Cloud через одноплатный компьютер	213
• Подключение камер к Insentry.Cloud с помощью Insentry.Watch	216
• Подключение камер к Insentry.Cloud с помощью Insentry.Bridge	218
• Подключение к Insentry.Cloud камер с публичным IP	222
• Управление подпиской	224
• Запись и хранение архива в облаке	225
• Управление учётными записями	226
• Отключение камер от облака	227

О системе Insentry

Программный комплекс Insentry предназначен для видеонаблюдения за обстановкой, автоматического обнаружения нештатных ситуаций и оповещения о событиях, представляющих возможную угрозу безопасности на обозреваемой территории.

Основные функции Insentry:

- обзорное видеонаблюдение в реальном времени;
- видеоаналитика и оповещения о событиях и угрозах безопасности;
- запись видеоархива локально и в облако;
- формирование аналитических отчётов;
- управление доступом пользователей к камерам и данным.

Поддерживаются аудиокодеки AAC, G.711.

Работа с ПО Insentry и все настройки выполняются через веб-клиент или мобильное приложение (см. *Руководство пользователя*, раздел *Мобильная версия Insentry*).

Чтобы начать использовать серверную версию Insentry, нужно [получить лицензию на сайте insentry.video](#). Для использования облачной версии Insentry необходимо [оформить подписку на сайте insentry.video](#).

Системные требования

К серверу

Требования к серверу, на котором развёрнуто ПО Insentry, зависят от количества подключенных камер и сценариев использования системы. Для расчёта подходящих параметров сервера воспользуйтесь [калькулятором на сайте insentry.io](#) или [напишите в службу поддержки](#).

К рабочим местам

Процессор	Не ниже Intel Core i7 с тактовой частотой 3,5 ГГц
Оперативная память	Не менее 16 ГБ
Хранилище	SSD не менее 512 ГБ
Видеокарта	Nvidia GeForce GTX 1050 и старше с поддержкой CUDA
Сетевой адаптер	Gigabit Ethernet
Монитор	17'', с разрешением 1920x1080 пикселей и выше
Операционная система	Windows: Windows 10 и старше. Linux: CentOS 7 и старше, RHEL 7.x и старше, Ubuntu
Архиватор	7zip или другой, поддерживающий работу с zip архивами
Браузер	Google Chrome последней версии

К камерам

Стандарт сжатия видеоданных	H.264, H.265
Поддержка сетевых протоколов	Fast Ethernet, Gigabit Ethernet, IEEE 802.11
Поддержка протоколов обмена данными	ONVIF, RTSP/RTP
Разрешение	До 16 Мп
Прочее	Поддержка настройки периода отправки ключевых кадров

Внимание! Для поддержки видеокodeка H.265 требуется аппаратное ускорение браузера и соответствие аппаратного обеспечения техническим требованиям, необходимым для работы с кодеком H.265.

Установка и обновление ПО Insentry

Для установки, обновления, переустановки и удаления ПО Insentry используется единый инсталлятор, который можно скачать на сайте insentry.video после получения лицензии.

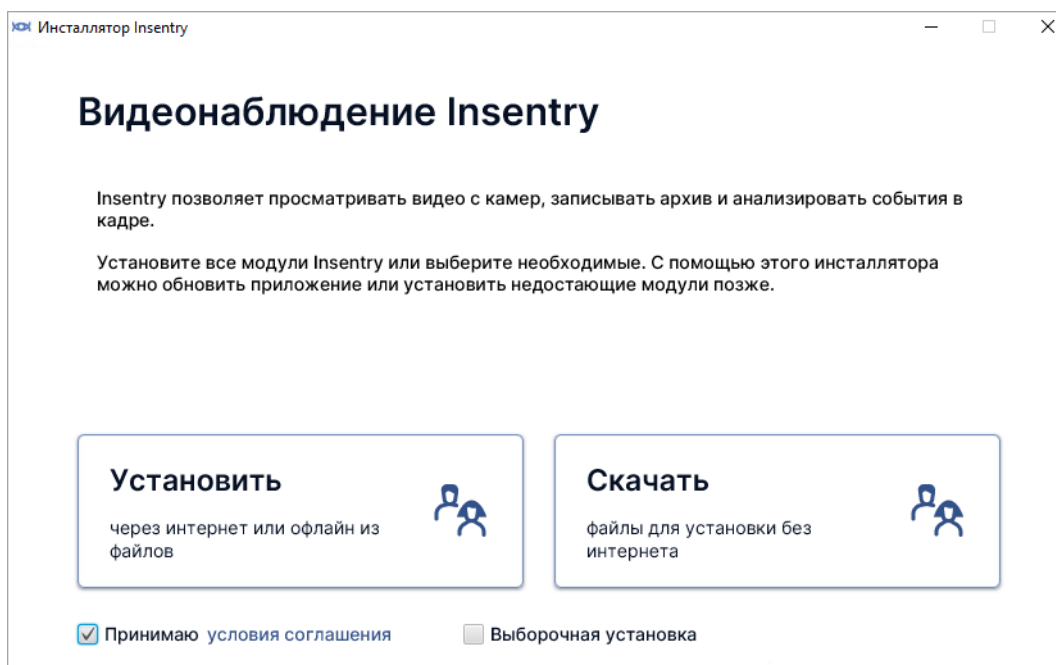
Установка ПО Insentry

Установка ПО Insentry на Windows

Внимание! Для корректной работы видеоаналитики скачайте и установите драйверы видеокарты с поддержкой Cuda с сайта NVidia (не из центра обновлений Windows).

Запуск инсталлятора

- Зарегистрируйтесь и получите лицензию на сайте insentry.video.
- В разделе **Личный кабинет** → **Мои лицензии** на сайте insentry.video/ перейдите в настройки лицензии и нажмите кнопку **Скачать дистрибутив**.
- Скачайте и запустите файл инсталлятора. Будет представлен начальный экран установки.
- Прочтите [условия соглашения](#) и если вы принимаете их, то установите отметку.



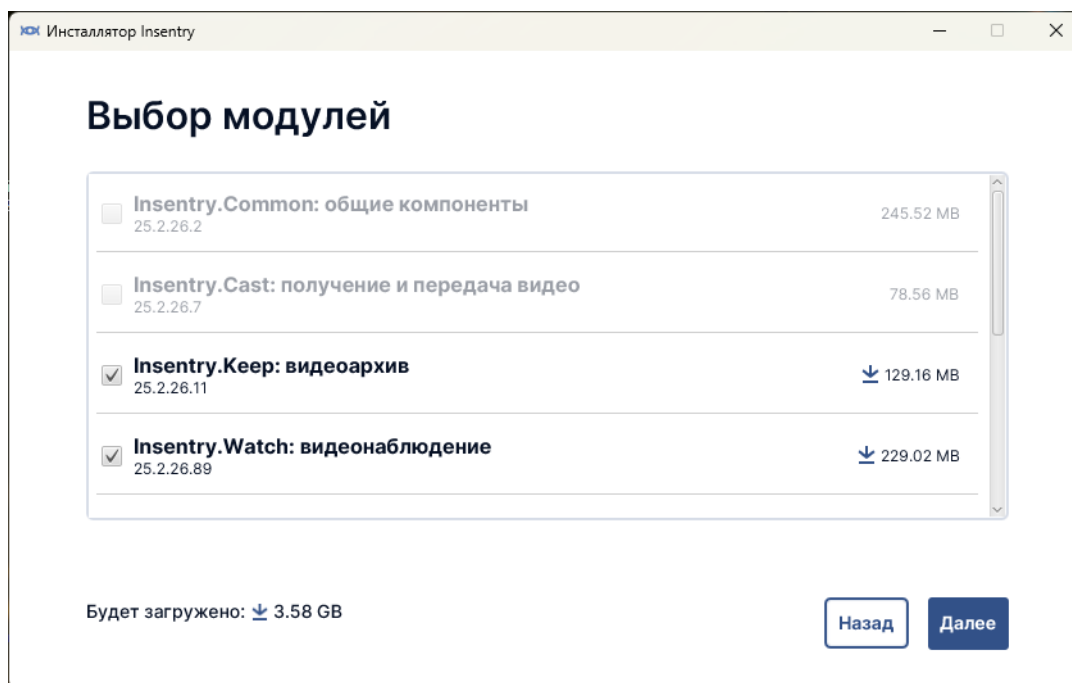
Insentry можно установить через интернет или [офлайн](#). Для офлайн установки потребуется заранее скачать установочные файлы и перенести их на сервер, где будет установлено ПО Insentry.

Есть два варианта установки ПО Insentry: полная и выборочная. [Выборочная установка](#) используется, если какие-то из модулей ПО Insentry пока не нужны. Их можно установить позже с помощью этого же инсталлятора.

Скачивание установочных файлов

Установочные файлы нужны, чтобы установить Insentry без интернета.

Чтобы скачать файлы, выберите раздел **Скачать** на главном экране установки Insentry.



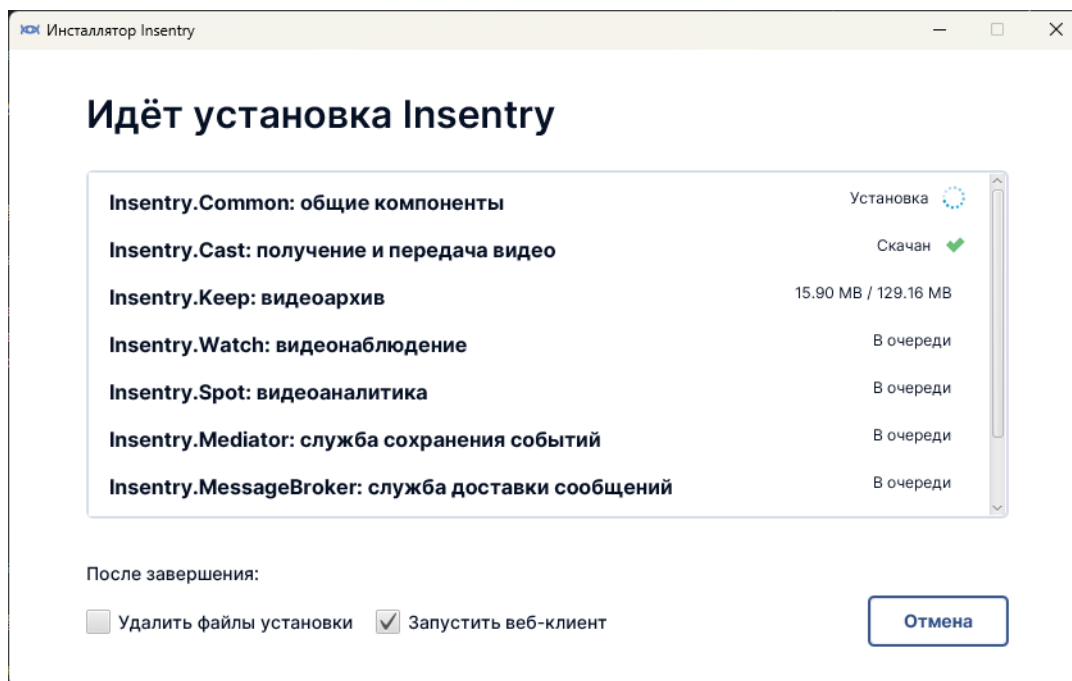
Выберите модули, установочные файлы для которых требуется скачать, и нажмите **Далее**.

Процесс загрузки будет отображаться в окне. После завершения загрузки установочные файлы выбранных модулей будут в папке distrib там же, где лежит файл инсталлятора. Перенесите эту папку на сервер, где будет установлено ПО Insentry, чтобы установить там Insentry офлайн.

Полная установка

Для полной установки Insentry требуется подключение к интернету.

Нажмите кнопку **Установить** на начальном экране установки. Начнётся процесс установки Insentry.



Чтобы удалить скачанные при установке файлы, установите отметку **Удалить файлы установки**. Если потребуется, их можно будет скачать позже с помощью этого же инсталлятора.

Выборочная установка

Онлайн-режим

Установите отметку **Выборочная установка** на начальном экране инсталлятора и нажмите кнопку **Установить**.

Будет представлен список модулей системы. Выберите, какие модули установить. В нижней части окна будет показано, сколько данных будет загружено и сколько потребуется места на диске для установки отмеченных модулей.

Нажмите **Далее**. Начнётся установка выбранных модулей, будет показан ход установки каждого модуля.

Офлайн-режим

Офлайн установка используется для установки Insentry на серверах, которые не подключены к интернету. В этом случае:

1. Заранее скачайте установочные файлы и положите их в папку distrib рядом с файлом инсталлятора на сервере, где будет установлено ПО Insentry.
2. Запустите инсталлятор в режиме выборочной установки.
3. Установите отметку **Только доступные без интернета**. В списке останутся только те модули, установочные файлы для которых есть в дистрибутиве. Набор файлов может отличаться в зависимости от версии скачанного дистрибутива.
4. Завершите установку.

Установка ПО Insentry на Linux

Установка видеонаблюдения Insentry на CentOS Linux с помощью Docker

1. Настройте системные SSD-серверы в RAID1 средствами встроенного RAID-контроллера.
2. Установите CentOS 7.8. При разметке используйте ручное распределение разделов и не выделяйте под /home отдельный раздел: отдайте всё доступное место под "/.
3. Присвойте серверу статический IP командой `sudo nmtui`

Внимание! В nmtui для основного сетевого интерфейса сервера в параметре **IPv4 CONFIGURATION** укажите режим **Manual**. Это важно, иначе потом будут проблемы в kubernetes.

4. Установите необходимые пакеты:

```
sudo yum install gcc gcc-c++ wget mc nano pciutils lshw git autoconf
automake bzip2 bzip2-devel cmake freetype-devel libtool make mercurial
pkgconfig zlib-devel traceroute unzip -y
```

5. Добавьте имя и IP сервера в файл /etc/hosts командой `sudo nano /etc/hosts`

Пример: 192.168.0.10 insentryserver

6. Измените имя сервера на прописанное в /etc/hosts: `sudo nmtui`

7. Установка Java 8 и Java 11:

```
sudo yum install java-1.8.0-openjdk-devel
sudo yum install java-11-openjdk-devel
```

8. Установка docker-ce:

```
sudo yum install -y yum-utils device-mapper-persistent-data lvm2
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
sudo yum install -y docker-ce
```

9. Добавление прав пользователю admin на использование docker:

```
sudo usermod -aG docker admin
```

10. Запуск docker и установка автозагрузки службы.

```
sudo systemctl enable docker
sudo systemctl start docker
```

11. Создание отдельного тома для хранения данных

```
sudo docker volume create --name insentry-data
```

12. Проверьте порты, необходимые для работы Insentry:

```
netstat -ln | grep ':3301\|:3291\|:3297\|:3299\|:5540\|:9200\|:7560\|:8008
\|:8520\|:8530\|:8535\|:9350\|:8081'
```


Запустите Docker. Существует две версии приложения Insentry:

13.
 - **Release** - для рабочих серверов,
 - **Snapshot** для тестирования новых возможностей.

Внимание! Работоспособность Snapshot сборки не гарантирована. Поддержка осуществляется только для Release сборки.

Команда для запуска Docker для Release сборки в полном виде:

Обратите внимание — строка запуска изменилась. Появились новые параметры `--privileged` `--cap-add=NET_ADMIN` .

```
sudo docker run \
--name insentry_watch \
--detach \
--restart unless-stopped \
--network host \
--volume insentry-data:/var/lib \
--volume /etc/timezone:/etc/timezone:ro \
--volume /etc/localtime:/etc/localtime:ro \
--privileged --cap-add=NET_ADMIN \
--device /dev/net/tun:/dev/net/tun \
--stop-timeout 60 \
cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/amd64:26.1.31.171
```

Для Snapshot сборки:

```
sudo docker run \
--name insentry_watch \
--detach \
--restart unless-stopped \
--network host \
--volume insentry-data:/var/lib \
--volume /etc/timezone:/etc/timezone:ro \
--volume /etc/localtime:/etc/localtime:ro \
--privileged --cap-add=NET_ADMIN \
--device /dev/net/tun:/dev/net/tun \
--stop-timeout 60 \
cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/amd64:latest
```

Проверьте работу контейнера:

```
sudo docker ps
```

При правильном выполнении Insentry Watch будет доступен по адресу хоста, порт 9200.

Установка видеонаблюдения Insentry на Ubuntu Linux с помощью Docker

- [Создание пользователя insentry](#)
- [Установка необходимых пакетов](#)
- [Запуск Docker образа Insentry](#)

Создание пользователя insentry

1. Создайте пользователя `insentry` с помощью команды `sudo adduser insentry`
Имя пользователя указывайте в нижнем регистре.
2. В появившихся строках укажите и подтвердите пароль.
3. При необходимости введите дополнительные данные учётной записи.
4. Дайте пользователю `insentry` права администратора командой `sudo usermod -aG sudo insentry`
5. Авторизуйтесь заново с данными учётной записи пользователя `insentry`.

Установка необходимых пакетов

1. Введите команды:

```
sudo apt-get update
sudo apt-get install ca-certificates curl gnupg lsb-release
```

2. Добавьте gpg-ключ:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg
--dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
```

3. Добавьте репозиторий Docker:

```
echo "deb [arch=$(dpkg --print-architecture)
signed-by=/usr/share/keyrings/docker-archive-keyring.gpg]
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" |
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

4. Обновите базу данных пакетов информацией о пакетах Docker из добавленного репозитория:

```
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io
```

5. Дать права пользователю системы на использование Docker:

```
sudo usermod -aG docker insentry
```

6. Запустите docker и включите автозагрузку службы:

```
sudo systemctl enable docker
sudo systemctl start docker
```

Запуск Docker образа Insentry

1. Создайте отдельный том для хранения данных:

```
sudo docker volume create --name insentry-data
```

2. Проверьте порты, необходимые для работы Insentry:

```
netstat -ln | grep ':3301\|:3291\|:3297\|:3299\|:5540\|:9200\|:7560\|:8008\|:8520\|:8530\|:8535\|:9350\|:8081'
```

Запустите Docker. Существует две сборки Insentry:

3.
 - **Release** - для рабочих серверов,
 - **Snapshot** для тестирования новых возможностей.

Обратите внимание — строка запуска изменилась. Появились новые параметры `--privileged` `--cap-add=NET_ADMIN`.

Команда для запуска Docker для Release сборки:

```
sudo docker run \
--name insentry_watch \
--detach \
--restart unless-stopped \
--network host \
--volume insentry-data:/var/lib \
--volume /etc/timezone:/etc/timezone:ro \
--volume /etc/localtime:/etc/localtime:ro \
--privileged --cap-add=NET_ADMIN \
--device /dev/net/tun:/dev/net/tun \
--stop-timeout 60
cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/amd64:26.1.31.171
```

Для Snapshot сборки:

```
sudo docker run \
--name insentry_watch \
--detach \
--restart unless-stopped \
--network host \
--volume insentry-data:/var/lib \
--volume /etc/timezone:/etc/timezone:ro \
--volume /etc/localtime:/etc/localtime:ro \
--privileged --cap-add=NET_ADMIN \
--device /dev/net/tun:/dev/net/tun \
--stop-timeout 60 \
cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/amd64:latest
```

Внимание! Работоспособность Snapshot сборки не гарантирована. Поддержка осуществляется только для Release сборки!

1. Если вы используете отдельный диск для архива, смонтированный в каталог (например, `/mnt/video`) – подключите к контейнеру два volume:

```
sudo docker run \
  --name insentry_watch \
  --detach \
  --restart unless-stopped \
  --network host \
  --volume insentry-data:/var/lib \
  --volume /mnt/video:/mnt/video \
  --volume /etc/timezone:/etc/timezone:ro \
  --volume /etc/localtime:/etc/localtime:ro \
  --privileged --cap-add=NET_ADMIN \
  --device /dev/net/tun:/dev/net/tun \
  --stop-timeout 60 \
  cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/amd64:26.1.31.171
```

Затем [настройте доступ для модуля Keep](#) к этому каталогу — он будет доступен из контейнера по тому же пути, что виден в родительской системе – `/mnt/video`:

Local storage			
Диск	Объем диска	Свободно на диске	Каталог
/mnt/video/	1832 ГБ	1739 ГБ	/mnt/video/

2. Проверьте работу контейнера:

```
sudo docker ps
```

При правильном выполнении Insentry Watch будет доступен по адресу хоста, порт 9200.

Установка видеонаблюдения Insentry на Raspberry Pi 4B с помощью Docker

Ниже описана только установка видеонаблюдения. Видеоаналитика [устанавливается отдельно](#).

Системные требования

1. ОС 64х. Рекомендуемая ОС — Ubuntu 20.04.
2. 8 ГБ оперативной памяти на Raspberry. На 4 ГБ Insentry может работать нестабильно.

Установка Ubuntu 20.04 на Raspberry Pi

Для установки на Raspberry Pi Ubuntu 20.04 используйте [официальную англоязычную инструкцию](#) или [одну из русскоязычных инструкций](#).

Создание пользователя insentry

1. Создайте учётную запись insentry с помощью команды `sudo adduser insentry`
Имя пользователя указывайте в нижнем регистре.
2. В появившихся строках укажите и подтвердите пароль.
3. При необходимости введите дополнительные данные учётной записи.

4. Дайте пользователю *insentry* права администратора командой `sudo usermod -aG sudo insentry`
5. Авторизуйтесь заново с данными учётной записи пользователя *insentry*.

Установка необходимых пакетов

1. Введите команды:

```
sudo apt-get install aptitude
sudo aptitude install apt-transport-https ca-certificates curl gnupg-agent
software-properties-common
```

2. Добавьте gpg-ключ:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add
-
```

3. Добавьте репозиторий Docker:

```
sudo add-apt-repository "deb [arch=arm64]
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
```

4. Обновите базу данных пакетов информацией о пакетах Docker из добавленного репозитория:

```
sudo aptitude update
sudo aptitude install docker-ce
```

5. Дать права пользователю системы на использование Docker:

```
sudo usermod -aG docker insentry
```

6. Запустите docker и включите автозагрузку службы:

```
sudo systemctl enable docker
sudo systemctl start docker
```

Запуск Docker образа Insentry

1. Создайте отдельный том для хранения данных:

```
sudo docker volume create --name insentry-data
```

2. Убедитесь, что на хосте свободны порты 80, 554, 9200:

```
sudo netstat -ln
```

Запустите Docker. Существует две сборки Insentry:

3.
 - Release - для рабочих серверов,
 - Snapshot для тестирования новых возможностей.

Обратите внимание — строка запуска изменилась. Появились новые параметры `--privileged` `--cap-add=NET_ADMIN` .

Команда для запуска Docker для Release сборки:

```
sudo docker run \
--name insentry_watch \
--detach \
--restart unless-stopped \
--network host \
--volume insentry-data:/var/lib \
--privileged --cap-add=NET_ADMIN \
--device /dev/net/tun:/dev/net/tun \
--stop-timeout 60 \
cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/arm64:26.1.31.171
```

Для Snapshot сборки:

```
sudo docker run \
--name insentry_watch \
--detach \
--restart unless-stopped \
--network host \
--volume insentry-data:/var/lib \
--privileged --cap-add=NET_ADMIN \
--device /dev/net/tun:/dev/net/tun \
--stop-timeout 60 \
cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/arm64:latest
```

Внимание! Работоспособность Snapshot сборки не гарантирована. Поддержка осуществляется только для Release сборки!

1. Если вы используете отдельный диск для архива, смонтированный в каталог (например, `/mnt/video`) – подключите к контейнеру два volume:

```
sudo docker run \
--name insentry_watch \
--detach \
--restart unless-stopped \
--network host \
--volume insentry-data:/var/lib \
--volume /mnt/video:/mnt/video \
--privileged \
--cap-add=NET_ADMIN \
--device /dev/net/tun:/dev/net/tun \
--stop-timeout 60 \
cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/arm64:26.1.31.171
```

Затем [настройте доступ для модуля Keep](#) к этому каталогу — он будет доступен из контейнера по тому же пути, что виден в родительской системе – `/mnt/video`:

Local storage			
Диск	Объем диска	Свободно на диске	Каталог
/mnt/video/	1832 ГБ	1739 ГБ	/mnt/video/

2. Проверьте работу контейнера:

```
sudo docker ps
```

При правильном выполнении Insentry Watch будет доступен по адресу хоста, порт 9200.

Установка видеоаналитики на Ubuntu Linux

Для подключения видеоаналитики необходимо установить дополнительный контейнер со службой Spot. Ниже описана только установка видеоаналитики. Видеонаблюдение [устанавливается отдельно](#).

Для работы интеллектуальных детекторов службы Spot необходима видеокарта Nvidia не ниже GeForce 1050 Ti с установленными драйверами. Базовый детектор движения может работать и без видеокарты.

Обновление службы Insentry Spot до версии 22.2 и выше

Для обновления службы Insentry Spot до версии 22.2 и выше, необходимо выполнить обновление службы Watch до версии 22.2 или выше. Для обновления служб Insentry Watch и Spot до версии 22.2 и выше необходимо выполнить следующие действия: 1. Остановить и удалить работающие контейнеры Watch и Spot. 2. Запустить контейнер с Insentry Watch версии 22.2 или выше. 3. Запустить контейнер с Insentry Spot версии 22.2 или выше.

Начиная с версии 22.2 останавливать контейнеры для их обновления не нужно.

Проверьте наличие драйверов видеокарты и установите их, если нужно.

```
nvidia-smi -L
```

Команда для установки драйверов Nvidia:

```
sudo apt install nvidia-driver-535-server
```

Установите Nvidia Container Runtime (вводить построчно):

```
curl -s -L https://nvidia.github.io/nvidia-container-runtime/gpgkey | \
sudo apt-key add -
distribution=$(. /etc/os-release;echo $ID$VERSION_ID)
curl -s -L https://nvidia.github.io/nvidia-container-runtime/$distribution/nvidia-container-runtime.list | \
sudo tee /etc/apt/sources.list.d/nvidia-container-runtime.list
sudo apt-get update
sudo apt-get install nvidia-container-runtime
```

Перезпустите docker:

```
sudo systemctl stop docker
sudo systemctl start docker
```

Во избежание проблем с обновлением драйверов nvidia во время работы контейнера, выполните следующую команду:

```
yes | sudo apt purge unattended-upgrades
```

Установите новый контейнер со службой Spot. Ключ `-gpus all` включает поддержку видеокарт для контейнера. Если видеокарт несколько, то можно задавать определенную с помощью индекса `-gpus i`, где `i` это порядковый номер видеокарты. Узнать порядковый номер видеокарты можно с помощью команды `nvidia-smi -L`

Запустите Docker. Существует две сборки Insentry:

- **Release** — для рабочих серверов,
- **Snapshot** — для тестирования новых возможностей.

Внимание! Работоспособность Snapshot сборки не гарантирована. Поддержка осуществляется только для Release сборки.

Команда для Release сборки:

```
sudo docker run \
--name insentry_spot \
--detach \
--restart unless-stopped \
--network host \
--gpus all \
--shm-size=2gb \
--volume insentry-data:/var/lib \
--volume /etc/timezone:/etc/timezone:ro \
--volume /etc/localtime:/etc/localtime:ro \
cr.yandex/crp5a5q503oamalo3iou/insentry-spot/linux/amd64:26.1.31.26
```

Команда для Snapshot сборки:

```
sudo docker run \
--name insentry_spot \
--detach \
--restart unless-stopped \
--network host \
--gpus all \
--shm-size=2gb \
--volume insentry-data:/var/lib \
--volume /etc/timezone:/etc/timezone:ro \
--volume /etc/localtime:/etc/localtime:ro \
cr.yandex/crp5a5q503oamalo3iou/insentry-spot/linux/amd64:latest
```

Установка видеоаналитики Insentry на Raspberry Pi 4B

Для подключения видеоаналитики необходимо установить дополнительный контейнер со службой Spot. Ниже описана только установка видеоаналитики. Видеонаблюдение [устанавливается отдельно](#).

Для работы интеллектуальных детекторов службы Spot необходима видеокарта Nvidia не ниже GeForce 1050 Ti с установленными драйверами и модуль TPU. Служба видеоаналитики тестировалась на [Google Coral](#) и [Intel Movidius 2](#). Работоспособность на других аналогичных устройствах не гарантируется.

- [Установка драйвера Coral](#)
- [Установка драйвера Movidius](#)
- [Установка контейнера со службой Spot](#)

Установка драйвера Coral

1. Добавьте репозиторий:


```
echo "deb https://packages.cloud.google.com/apt coral-edgetpu-stable main"
| sudo tee /etc/apt/sources.list.d/coral-edgetpu.list
curl https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo apt-key
add -
sudo apt-get update
```

2. Установите драйверы из добавленного репозитория:

```
sudo apt-get install gasket-dkms libedgetpu1-std
```

3. Добавьте группу apex и пользователя в неё:

```
sudo sh -c "echo 'SUBSYSTEM==\"apex\", MODE=\"0660\", GROUP=\"apex\"' >>
/etc/udev/rules.d/65-apex.rules"
sudo groupadd apex
sudo adduser $USER apex
```

4. Перезагрузите систему.

5. Проверьте доступность модуля:

```
lspci -nn | grep 089a
```

Ожидаемый ответ выглядит так: 03:00.0 System peripheral: Device 1ac1:089a

Источник: <https://coral.ai/docs/m2/get-started/#2a-on-linux>

Установка драйвера Movidius

Для установки компонентов (Movidius Neural Compute SDK) для работы с Movidius рекомендуется использовать SD-карту не менее 16 ГБ. Для успешной установки Movidius Neural Compute SDK рекомендуется увеличить файл подкачки со 100 до 1024 МБ или больше.

1. Откройте файл dphys-swapfile и измените строку "CONF_SWAPSIZE=100" на "CONF_SWAPSIZE=1024" :

```
sudo nano /etc/dphys-swapfile
```

2. Перезапустите службу файла подкачки:

```
sudo /etc/init.d/dphys-swapfile restart
```

3. Установите Movidius Neural Compute SDK:

```
git clone -b ncsdk2 http://github.com/Movidius/ncsdk && cd ncsdk && make
install
```

4. Для установки Movidius Neural Compute SDK версии 1.x воспользуйтесь командой:

```
git clone http://github.com/Movidius/ncsdk && cd ncsdk && make install
```

Внимание! Версии Movidius Neural Compute SDK 1.x и 2.x не имеют обратной совместимости.

Источник: <https://movidius.github.io/ncsdk/install.html>

Установка нового контейнера со службой Spot

Существует две сборки Insentry:

- **Release** — для рабочих серверов,
- **Snapshot** — для тестирования новых возможностей.

Внимание! Работоспособность Snapshot сборки не гарантирована. Поддержка осуществляется только для Release сборки.

Команда для Release сборки:

```
docker run --name insentry_spot --detach --restart always --network host
--volume insentry-data:/var/lib --privileged --volume
/dev/bus/usb:/dev/bus/usb --volume /etc/timezone:/etc/timezone:ro --volume
/etc/localtime:/etc/localtime:ro
cr.yandex/crp5a5q503oamalo3iou/insentry-spot/linux/arm64:26.1.31.26
```

Команда для Snapshot сборки:

```
docker run --name insentry_spot --detach --restart always --network host
--volume insentry-data:/var/lib --privileged --volume
/dev/bus/usb:/dev/bus/usb --volume /etc/timezone:/etc/timezone:ro --volume
/etc/localtime:/etc/localtime:ro
cr.yandex/crp5a5q503oamalo3iou/insentry-spot/linux/arm64:latest
```

Установка модуля Get для интеграции с внешними системами

Служба Get включена в устанавливаемый контейнер Watch. Если необходимо установить контейнер со службой Get на отдельный сервер, используйте следующую команду:

```
sudo docker run \
--name get \
--detach \
--restart unless-stopped \
--network host \
--volume insentry-data:/var/lib \
cr.yandex/crp5a5q503oamalo3iou/get_release/linux/amd64:26.1.31.11
```

Обновление ПО Insentry

- [B Linux](#)
- [B Windows](#)

Если конфигурационные файлы были изменены при участии технической поддержки, то перед обновлением обязательно свяжитесь с технической поддержкой, чтобы не потерять внесённые изменения.

Перед обновлением [выполните бэкап настроек](#).

В Linux

1. Удалите контейнер командой `sudo docker stop rm [ИМЯ_КОНТЕЙНЕРА]`
2. Запустите новый контейнер с ссылкой на новый образ.

Обратите внимание — строка запуска изменилась. Появились новые параметры `--privileged` `--cap-add=NET_ADMIN` .

```
sudo docker run \
--name insentry_watch \
--detach \
--restart unless-stopped \
--network host \
--volume insentry-data:/var/lib \
--volume /mnt/video:/mnt/video \
--privileged \
--cap-add=NET_ADMIN \
--device /dev/net/tun:/dev/net/tun \
--stop-timeout 60 \
cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/amd64:26.1.31.171
```

Важно! Если вы вносили измерения в первоначальную команду для запуска контейнера, то последующие запуски новых контейнеров следует выполнять используя те же параметры команды `docker run` .

1. Проверьте работу контейнера командой `sudo docker ps`

После обновления Insentry Watch вы можете использовать старый образ для восстановления предыдущей версии Insentry Watch или удалить старый образ. Для удаления старого образа выполните команду `sudo docker image rm [ID_СТАРОГО_ОБРАЗА]` . При удалении образа может возникнуть ошибка:

```
Error response from daemon: conflict: unable to delete 42b846670db0 (must be forced) -
image is being used by stopped container 3d236abd9e19
```

Для её решения выполните принудительное удаление образа используя флаг `-f` . Пример:
`sudo docker image rm -f 42b846670db0` .

Посмотреть список всех образов можно с помощью команды `sudo docker images` .

Для восстановления прежней версии проделайте аналогичные шаги, что и при обновлении. Для запуска контейнера вы можете использовать ссылку на старый образ или его ID.

Для обновления Insentry Spot необходимо проделать аналогичные действия, используя команду для запуска контейнера InsentrySpot и [ссылку на новую версию образа Insentry Spot](#).

В Windows

Общие сведения

Для обновления компонентов Insentry версии 21.3 и выше используется тот же инсталлятор, с помощью которого было установлено приложение. Можно использовать тот же самый файл или скачать новый на сайте <https://insentry.io/>.

Так же как и при установке, ПО Insentry можно обновить полностью или выборочно.

Полное обновление требует подключения к интернету сервера, на котором обновляется ПО InSentry. Если на сервере нет подключения к интернету, то используйте офлайн-режим, чтобы обновить компоненты из заранее скачанного дистрибутива.

Выборочное обновление используется, если какие-то из компонент ПО InSentry пока не требуется обновлять. Их можно обновить позже или удалить.

Запуск обновления

Чтобы обновить модули InSentry, запустите инсталлятор и нажмите кнопку **Обновить**. Кнопка неактивна, если обновлений нет.

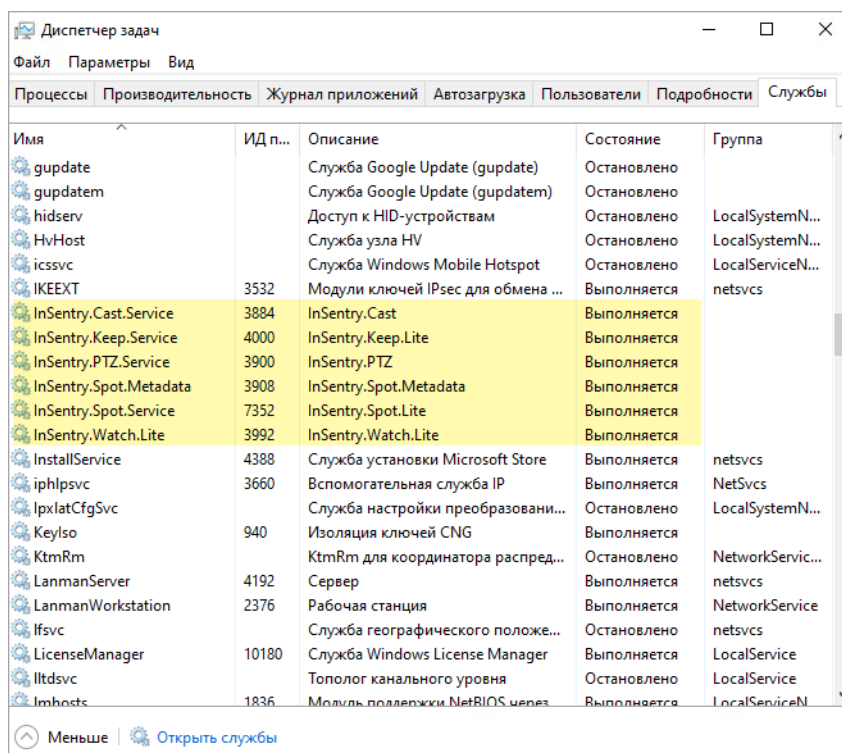
Наличие более свежих версий модулей проверяется онлайн, а если подключения к интернету нет, то в папке distrib там же, где находится файл инсталлятора. Поместите в эту папку заранее скачанные свежие версии модулей, чтобы обновить InSentry без подключения к интернету.

Проверка работоспособности модулей

Для проверки работы модулей после обновления, перейдите в раздел **Управление → Модули**.

В таблице показан статус работы каждого модуля.

Если модуль не работает, проверьте, что запущена соответствующая служба (**Диспетчер задач → Службы**).



Имя	ID п...	Описание	Состояние	Группа
gupdate		Служба Google Update (gupdate)	Остановлено	
gupdatem		Служба Google Update (gupdatem)	Остановлено	
hidserv		Доступ к HID-устройствам	Остановлено	LocalSystemN...
HvHost		Служба узла HV	Остановлено	LocalSystemN...
icssvc		Служба Windows Mobile Hotspot	Остановлено	LocalServiceN...
IKEEXT	3532	Модули ключей IPsec для обмена ...	Выполняется	netsvcs
InSentry.Cast.Service	3884	InSentry.Cast	Выполняется	
InSentry.Keep.Service	4000	InSentry.Keep.Lite	Выполняется	
InSentry.PTZ.Service	3900	InSentry.PTZ	Выполняется	
InSentry.Spot.Metadata	3908	InSentry.Spot.Metadata	Выполняется	
InSentry.Spot.Service	7352	InSentry.Spot.Lite	Выполняется	
InSentry.Watch.Lite	3992	InSentry.Watch.Lite	Выполняется	
InstallService	4388	Служба установки Microsoft Store	Выполняется	netsvcs
iphlpvc	3660	Вспомогательная служба IP	Выполняется	NetSvcs
IpmlatCfgSvc		Служба настройки преобразовани...	Остановлено	LocalSystemN...
KeyIso	940	Изоляция ключей CNG	Выполняется	
KtmRm		KtmRm для координатора распредел...	Остановлено	NetworkServic...
LanmanServer	4192	Сервер	Выполняется	netsvcs
LanmanWorkstation	2376	Рабочая станция	Выполняется	NetworkService
Ifsvc		Служба географического полож...	Остановлено	netsvcs
LicenseManager	10180	Служба Windows License Manager	Выполняется	LocalService
Iltdsvc		Тополог канального уровня	Остановлено	LocalService
Imhosts	1836	Модуль поддержки NetBIOS через	Выполняется	LocalServiceN

Обновление через командную строку

Существует возможность обновить модули InSentry в фоновом режиме через консоль.

Синтаксис команд:

- `/path/insentry-installer.exe update` – обновить все установленные компоненты, лог обновления писать в txt файл.
- `/path/insentry-installer.exe prepare keep` – загрузить последнюю сборку модуля Кеер, положить в каталог.

Вместо path укажите путь до файла инсталлятора insentry-installer.exe.

Логи пишутся в %temp% с начала запуска.

Переустановка ПО Insentry

- [B Linux](#)
- [B Windows](#)

Перед переустановкой [выполните бэкап базы данных и настроек](#).

В Linux

Перед переустановкой ПО Insentry необходимо выполнить удаление контейнера Docker и при необходимости удалить Volume контейнера.

1. Остановите контейнер командой

```
sudo docker stop --time=60 [ИМЯ_КОНТЕЙНЕРА]
```

Если имя вашего контейнера отличается, то посмотреть запущенные контейнеры можно с помощью команды `sudo docker ps`. Для просмотра всех контейнеров выполните эту команду с флагом `-a`: `sudo docker ps -a`

2. Запомните имя или ID контейнера, оно еще понадобится для его удаления:

```
sudo docker rm [ИМЯ ИЛИ ID КОНТЕЙНЕРА]
```

3. Удалите контейнер insentry_watch: `sudo docker rm insentry_watch`

4. При необходимости можно удалить volume контейнера. В этом случае удаляться все настройки программы (логины и база данных).

```
sudo docker volume rm insentry-data
```

Ошибка вида **Error response from daemon: remove insentry-data: volume is in use - [e1b36ea2c9e15e52e786e4567bcc778cd984d37f49a61809518f57ed8d962a48, 56ac7277c93ca4cc5161301d942af091f06558919dabc9cc5501194ccb51ac7b]** означает, что Volume используется другими контейнерами. В квадратных кавычках перечисляются ID контейнеров, которые используют данный Volume. Первые цифры ID можно использовать для управления контейнерами. Для устранения проблемы контейнеры, указанные в ошибке, необходимо остановить и удалить:

```
sudo docker stop --time=60 [ИМЯ_КОНТЕЙНЕРА]
sudo docker rm [ID КОНТЕЙНЕРА]
```

5. Также вы можете удалить Image, которые не собираетесь больше использовать. Для просмотра всех Image воспользуйтесь командой:

```
sudo docker images
```

6. Для удаления контейнера воспользуйтесь командой:

```
sudo docker image rm -f [ID Image]
```

7. После удаления контейнера, Volume и Image можно заново установить Insentry:

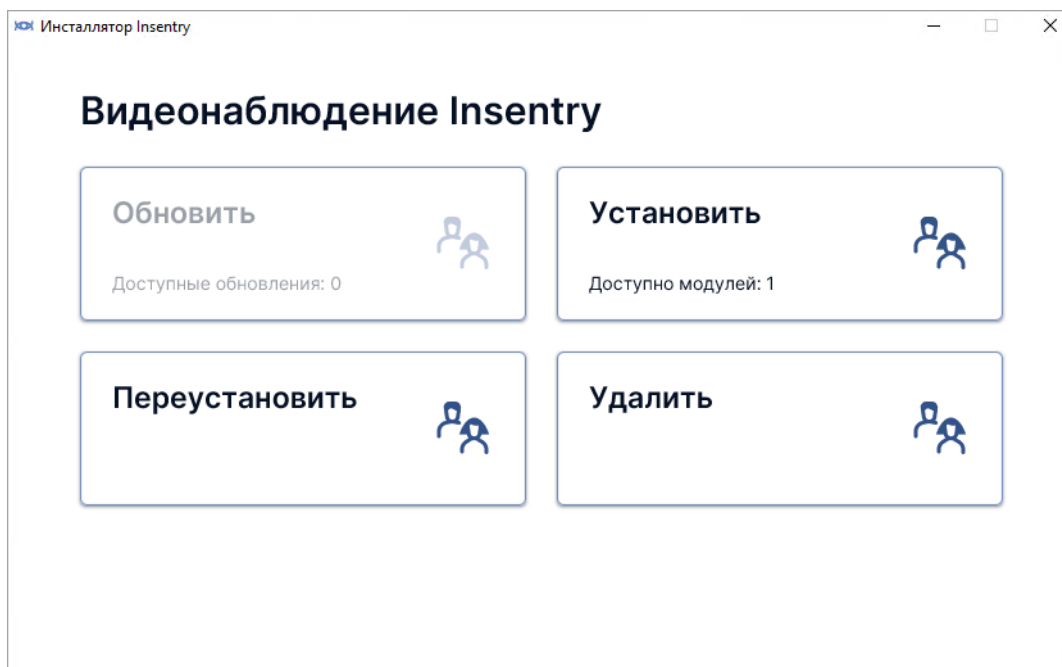
```
sudo docker run
--name insentry_watch
--detach
--restart unless-stopped
--network host
--volume insentry-data:/var/lib
--volume /etc/timezone:/etc/timezone:ro
--volume /etc/localtime:/etc/localtime:ro
--stop-timeout 60
cr.yandex/crp5a5q503oamalo3iou/insentry-watch/linux/amd64:26.1.31.171
```

8. После установки проверьте работу контейнера:

```
sudo docker ps
```

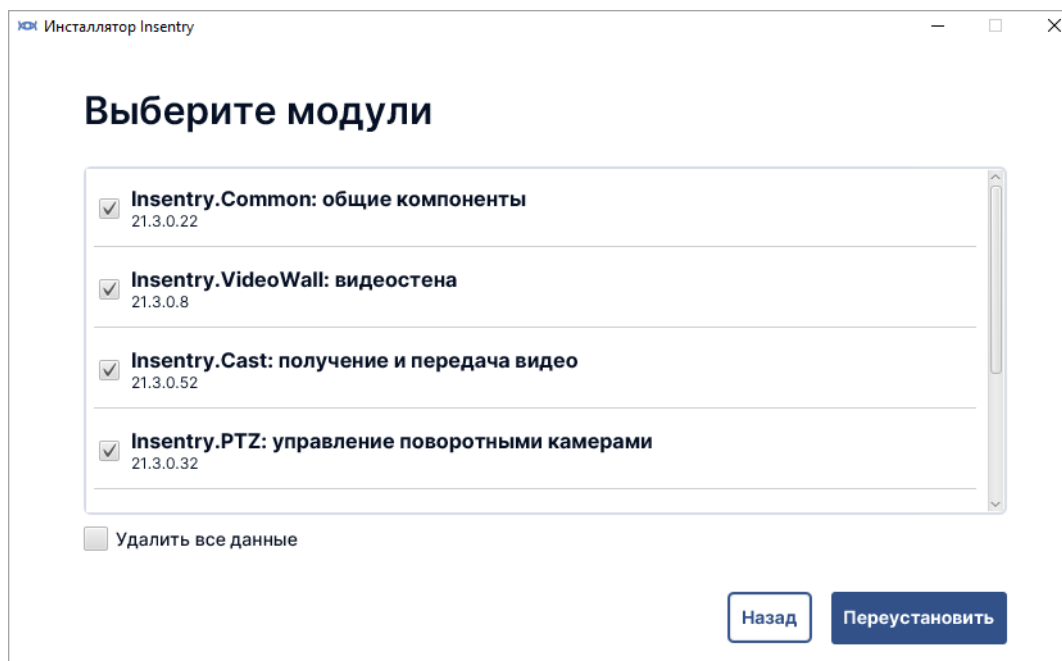
В Windows

Для переустановки Insentry используется тот же инсталлятор, что и для установки. Обновлять сам инсталлятор не нужно — достаточно просто запустить его в любой момент, когда потребуется переустановить, обновить Insentry или установить дополнительные модули. Скачать инсталлятор можно на сайте insentry.video в разделе **Мои лицензии**, выбрав лицензию в списке.



Чтобы переустановить Insentry, запустите инсталлятор и нажмите кнопку **Переустановить**. Все модули будут загружены по интернету, а в случае отсутствия подключения — из папки distrib там же, где находится файл инсталлятора, как и при [установке ПО Insentry](#).

Чтобы стереть все данные: настройки камер и системы, записанный архив — установите отметку **Удалить все данные**. Если отметка не установлена, то после переустановки настройки системы и записанные файлы архива будут сохранены.



Бэкап базы данных, лицензий и настроек

- [В Linux](#)
- [В Windows](#)

Вы можете сохранить файлы базы данных приложения, лицензий и настроек установленных модулей Insentry.

Рекомендуем делать бэкап перед переустановкой ПО Insentry, а также [при обновлении ПО Insentry](#), если в конфигурацию были внесены изменения.

В Linux

Файлы базы данных

База данных располагается в контейнере по пути `/var/lib/InSentry/Watch.Lite/watch.db.mv.db`. Копировать её можно с помощью команды:

```
sudo docker cp [ID или ИМЯ
контейнера]:/var/lib/InSentry/Watch.Lite/watch.db.mv.db
/home/admin/watch.db.mv.db
```

А для восстановления достаточно скопировать её обратно:

```
sudo docker cp /home/admin/watch.db.mv.db [ID или ИМЯ
контейнера]:/var/lib/InSentry/Watch.Lite/watch.db.mv.db
```

Файлы лицензий

Если в Insentry активирована лицензия, то для бэкапа нужно скопировать файлы **cloud.dat** и **activation.lic** в контейнере `/var/lib/InSentry/Watch.Lite/`.

Windows

Файлы базы данных

Файлы базы данных расположены в папке `C:\ProgramData\InSentry\Watch.Lite` (файлы **.db**) или другому пути, указанному в настройках Watch (в файле `application.properties` строка `spring.datasource.url.....`).

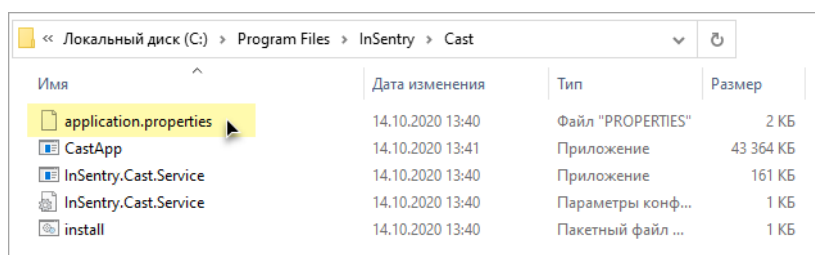
Файлы лицензий

Файлы лицензий **activation.lic** и **cloud.dat** расположены в папке `C:\ProgramData\InSentry\Watch.Lite`. Без них активация с тем же ключом невозможна.

Файлы с настройками

Чтобы сохранить настройки установленных модулей InSentry, скопируйте файлы **application.properties** для каждого модуля.

Эти файлы расположены в папках с названиями модулей в директории, куда установлено ПО InSentry. По умолчанию — `C:\Program Files\InSentry\папка модуля`.



Импорт настроек, лицензий и базы данных

- В Linux
- В Windows

Если вы делали **бэкап базы данных, лицензий и настроек**, то после переустановки InSentry нужно поместить файлы в нужные папки.

В Linux

Файлы базы данных

База данных располагается в контейнере по пути `/var/lib/InSentry/Watch.Lite/watch.db.mv.db`. Копировать её можно с помощью команды:

```
sudo docker cp [ID или ИМЯ
контейнера]:/var/lib/InSentry/Watch.Lite/watch.db.mv.db
/home/admin/watch.db.mv.db
```

А для восстановления достаточно скопировать её обратно:

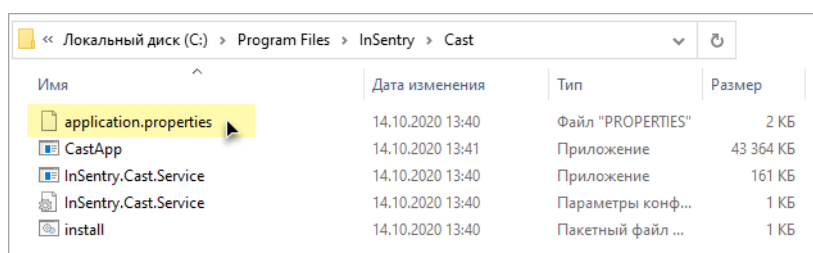

```
sudo docker cp /home/admin/watch.db.mv.db [ID или ИМЯ
контейнера]:/var/lib/InSentry/Watch.Lite/watch.db.mv.db
```

Файлы лицензий

Если в InSentry активирована лицензия, то для бэкапа нужно скопировать файлы **cloud.dat** и **activation.lic** в контейнере `/var/lib/InSentry/Watch.Lite/`.

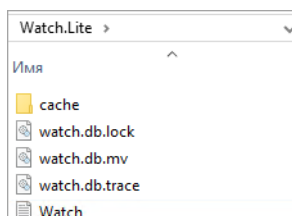
Windows

Файлы с настройками модулей расположены в папках с названиями модулей в директории, куда установлено ПО InSentry. По умолчанию — `C:\Program Files\InSentry\папка модуля`.



Файлы лицензий (*activation.lic* и *cloud.dat*) нужно поместить в папку `C:\ProgramData\InSentry\Watch.Lite`.

Файлы базы данных расположены в папке `C:\ProgramData\InSentry\Watch.Lite` (файлы **.db**) или там, где указано в настройках Watch (в файле *application.properties* строка *spring.datasource.url.....*).



Удаление ПО InSentry

- В Linux
- В Windows

В Linux

1. Остановите контейнер командой

```
sudo docker stop --time=60 [ИМЯ_КОНТЕЙНЕРА]
```

Если имя вашего контейнера отличается, то посмотреть запущенные контейнеры можно с помощью команды `sudo docker ps`. Для просмотра всех контейнеров выполните эту команду с флагом `-a`: `sudo docker ps -a`

2. Запомните имя или ID контейнера, оно еще понадобится для его удаления:

```
sudo docker rm [ИМЯ ИЛИ ID КОНТЕЙНЕРА]
```

3. Удалите контейнер insentry_watch: `sudo docker rm insentry_watch`
4. При необходимости можно удалить volume контейнера. В этом случае удалятся все настройки программы (логины и база данных).

```
sudo docker volume rm insentry-data
```

Ошибка вида **Error response from daemon: remove insentry-data: volume is in use - [e1b36ea2c9e15e52e786e4567bcc778cd984d37f49a61809518f57ed8d962a48, 56ac7277c93ca4cc5161301d942af091f06558919dabc9cc5501194ccb51ac7b]** означает, что Volume используется другими контейнерами. В квадратных кавычках перечисляются ID контейнеров, которые используют данный Volume. Первые цифры ID можно использовать для управления контейнерами. Для устранения проблемы контейнеры, указанные в ошибке, необходимо остановить и удалить:

```
sudo docker stop --time=60 [ИМЯ_КОНТЕЙНЕРА]
sudo docker rm [ID КОНТЕЙНЕРА]
```

5. Также вы можете удалить Image, которые не собираетесь больше использовать. Для просмотра всех Image воспользуйтесь командой:

```
sudo docker images
```

6. Для удаления контейнера воспользуйтесь командой:

```
sudo docker image rm -f [ID Image]
```

В Windows

Чтобы удалить ПО Insentry с компьютера, запустите инсталлятор и выберите пункт **Удалить**.

При переустановке и удалении Insentry есть возможность удалить также и данные: настройки камер и системы, записанный архив. Поставьте отметку **Удалить все данные**, чтобы всё стереть. Если отметка не установлена, то если вы удалите и потом поставите Insentry заново, настройки системы и записанные файлы архива будут сохранены.

Чтобы удалить Insentry в фоновом режиме через консоль, введите команду `/path/insentry-installer.exe --erasedata delete` – провести полное удаление всех компонент и пользовательских данных. Вместо path укажите путь до файла инсталлятора insentry-installer.exe.

Логи пишутся в `%temp%` с начала запуска.

Администрирование Insentry

Администрирование системы осуществляется в разделе **Управление**.

При переходе в раздел, первым представлен [список камер](#).

Камеры						Добавить камеру
Введите ваш запрос						🔍
Включить расширенный поиск						
Название / IP	Вендор / Модель	Потоки	Архив	Детекторы	Лицензия	
☐  AAC 172.17.17.17 PTZ	ONVIF onvif ptz camera	3			✓	
☐  Camera 1 172.17.17.17 PTZ	ONVIF onvif ptz camera	4	1		✓	
☐  Camera 2 172.17.17.17 PTZ	ONVIF onvif ptz camera	2			✓	
☐  Camera 3 172.17.17.17 PTZ	ONVIF onvif ptz camera	3			✓	
☐  Camera 4 172.17.17.17 PTZ	ONVIF onvif ptz camera	4		1	✓	
☐  Office 172.17.17.17 PTZ	ONVIF onvif ptz camera	1	1	1	✓	

Управление устройствами

В разделе **Управление → Устройства** вы можете подключить камеры к Insentry и настроить интеграцию с внешними системами, чтобы получать события от устройств, подключенных к ним.

Управление камерами

В разделе **Управление → Устройства → Камеры** вы можете подключить камеры к Insentry и настроить видеоаналитику.

Подключение камер к Insentry

Перед подключением к Insentry камеры и/или видеорегистраторы должны быть предварительно подключены к локальной сети.

Подключение камер автоматически и вручную

См. также: [Импорт и экспорт камер через файл](#)

Чтобы подключить камеру к Insentry, перейдите в раздел **Управление → Устройства → Камеры → Мастер добавления**. Откроется мастер добавления камер.

Мастер добавления камер

Обновить список

Камеры нет в списке

Учётные данные

Не выбрано

Логин

Пароль

Проверить подключение

☐	Название / IP	Вендор / Модель	Добавлено	HTTP	RTSP	ONVIF	PTZ	Протокол	Статус
☐	172.17.17.173	ONVIF onvif camera	0	80		80		ONVIF	
☐	172.17.17.173	Tantos TSi-Pn235FP	0	80				UPNP	
☐	172.17.17.173	ONVIF onvif camera	0	80		80		ONVIF	
☐	172.17.17.173	ONVIF onvif camera	0	80		80		ONVIF	
☐	172.17.17.173	Panasonic Other PTZ-model	0	80		80		ONVIF	
☐	172.17.17.173	Dahua DH-IPC-HDBW5431RP-ZE	0	80		80		ONVIF + UPNP	
☐	172.17.17.173	LTV CNE-640-48	0	80				UPNP	
☐	172.17.17.173	LTV CNE-650-41	0	80		80		ONVIF	
☐	172.17.17.173	Hikvision DS-2CD2655FWD-I2S	0	80				UPNP	

☐

Выбрано: 0/9

Добавить выбранные

Проверено: 0/9

Ошибки: 0/9

0/9

Insentry автоматически обнаруживает в локальной сети камеры, для которых выполнены следующие условия:

- на камере настроен профиль ONVIF;
- камера поддерживает протокол UPnP;
- на сетевом оборудовании локальной сети настроены сетевые службы для работы мультикаст трафика (если используется многоадресный режим трансляции видеопотоков с камер).

За пределами локального сегмента проверка выполняется по протоколу UPnP.

Обнаруженные камеры показаны в таблице. По каждой камере отображаются следующие данные:

- название или IP адрес;
- вендор и/или модель;
- количество раз, когда камера с таким адресом уже была добавлена в систему (столбец **Добавлено**);
- номера портов HTTP, RTSP, ONVIF;
- поддержка PTZ;
- протокол, по которому обнаружена камера;
- статус проверки подключения.

Таблицу можно сортировать по любому из признаков. Для сортировки нажмите на название заголовка столбца. Направление сортировки показано стрелкой.

Отметьте в списке камеры, которые собираетесь подключить, или выберите все, нажав на поле выбора слева от названия столбца **Название/IP**.

Если в списке нужной камеры или вы хотите добавить камеры с регистратора, нажмите **Камеры нет в списке** и [подключите камеру вручную](#).

Фильтрация списка обнаруженных камер

Для включения фильтрации нажмите кнопку фильтра справа от названия раздела в меню. Кнопка меняет вид в зависимости от состояния фильтра:



— есть активный фильтр;



— нет активных фильтров.

В верхней части рабочей области появится панель фильтрации. Фильтры настраиваются так же, как в других разделах системы.

Доступна фильтрация по следующим параметрам:

- типу камеры:
 - новые — ещё не добавленные в систему;
 - подключенные — камеры, которые были ранее подключены и добавлены в систему;
 - все;
- статусу проверки подключения.

Внимание! Данные не обновляются автоматически. После настройки фильтров необходимо нажать кнопку «Обновить»  для применения изменений.

Для удаления отдельного фильтра нажмите на «крестик» рядом с настроенным фильтром. Для сброса всех фильтров нажмите большой «крестик» в правой части панели фильтрации.

Если настроено несколько фильтров, будут показаны записи, удовлетворяющие настройкам всех фильтров.

Проверка подключения

Чтобы продолжить, укажите логин и пароль в полях в верхней части списка и нажмите кнопку **Проверить подключение**. Выбранные камеры будут опрошены с введенными данными (логинем и паролем). Результат проверки будет показан в столбце **Статус**. Камеры, которые успешно прошли проверку подключения, готовы к добавлению в систему.

Для удобства вы можете сохранить пару логин-пароль и подставлять нужные учетные данные для проверки камер. Для сохранения введенных логина и пароля нажмите на кнопку сохранения справа от поля пароль. Укажите название, под которым будут сохранены указанные данные. В дальнейшем вы сможете выбрать их из выпадающего списка **Учетные данные**.

Настройка подключения

Отметьте нужные камеры и нажмите **Добавить выбранные**.

В окне **Настройка подключения** вы можете:

1. Настроить шаблон названия для добавления подключаемых камер в систему. Для этого укажите название камер в поле **Шаблон названия**. Камеры будут добавлены в систему с указанным названием и пронумерованы последовательно, начиная со значения, указанного в поле **Начальное значение** (по умолчанию — 1). Например: «Камера 1», «Камера 2» и так далее.
2. Указать расположение камеры, выбрав из списка (если справочник тегов и расположений уже заполнен).
3. Включить трансляцию потока камеры в облачную версию Insentry.

Все эти настройки можно будет изменить в настройках камеры после добавления.

Настройка подключения

Настройки будут применены ко всем выбранным камерам (2)

Начальное значение

1

Шаблон названия*

Камера

Камеры будут названы по шаблону: Название 1, Название 2 ... Название N

Расположение

Не выбрано

☐ Транслировать в Cloud

Отмена

Далее

Укажите данные и нажмите **Далее**.

Начнётся добавление камер. После окончания добавления будет показан отчёт — сколько камер добавлено успешно. Если камеру добавить не удалось — будет указана причина.

Ручное подключение

Если нужная камера отсутствует в списке автообнаружения, выберите ручное подключение, нажав кнопку **Камеры нет в списке**. Ручное подключение также используется для [добавления камер с видеорегистратора](#).

В открывшемся окне укажите:

- IP адрес камеры и порты для подключения;
- логин и пароль (доступен выбор из списка сохранённых учётных данных);
- вендора и модель камеры, если они определены неверно. От указанных вендора и модели зависят доступные функции камеры. Воспользоваться функциями, которые не поддерживаются в указанной модели камеры, через Insentry не получится.

При необходимости здесь вы можете также указать расположение добавляемой камеры и включить трансляцию в облако.

Настройка подключения

Название*

Камера 801

Расположение

Серверная / -1 этаж

Учётные данные

Не выбрано

Логин

Пароль

Вендор

ONVIF

Модель

onvif ptz camera

IP адрес*

192.168.13.77

HTTP

80

RTSP*

554

ONVIF

80

Транслировать в Cloud

Отмена

Далее

Укажите данные в полях и нажмите **Далее**. Начнётся добавление указанной камеры. После окончания добавления будет показан отчёт с результатом. Если камеру добавить не удалось — будет указана причина.

Импорт камер из файла конфигурации

Список камер с настройками можно загрузить из файла формата *.xlsx. В результате импорта камеры автоматически подключаются к Insentry с настройками, указанными в файле.

Файл импорта должен содержать листы **Cameras**, **Profiles**, **Recordings** и **Tags**. Первые строки листов содержат названия столбцов и могут быть произвольными. Импорт производится в разделе **Управление → Система → Импорт/Экспорт → Импорт конфигурации Insentry**. Там же можно скачать шаблон для заполнения списка камер.

Формат листа Cameras

На листе Cameras обязательные для заполнения столбцы:

- Название
- Хост
- Логин

Если хотя бы один из них не заполнен, вся строка будет считаться комментарием, а не информацией о камере.

Остальные столбцы заполнять необязательно. Пустые столбцы будут интерпретироваться со значениями по умолчанию.

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Название	Название камеры	Текстовое поле длиной от 1 до 250 символов. Допустимы символы кириллицы, все печатные символы ASCII	Поле обязательно для заполнения
Хост	Адрес камеры	IPv4 адрес или доменное имя камеры, порт — целое число от 1 до 65535, согласно спецификации	Поле обязательно для заполнения
Логин	Логин доступа к камере	От 1 до 50 символов, допустимы все печатные символы ASCII	Поле обязательно для заполнения
Пароль	Пароль доступа к камере	От 1 до 50 символов, допустимы все печатные символы ASCII	Пусто
Описание	Описание камеры	Текстовое поле длиной от 0 до 250 символов. Допустимы символы кириллицы, все печатные символы ASCII	Пусто
Вендор	Производитель камеры	Текстовое поле, значение должно содержать название одного из [поддерживаемых вендоров] либо значение Other	Onvif
Модель	Модель камеры	Модель камеры. Если модель неизвестна, напишите Other model или Other PTZ-model	
Канал	Канал (для импорта камер с регистратора)	Целое число	Пусто
Поддержка PTZ	Идентификатор поворотной камеры	1 — да, 0 — нет	0
Поддержка омывателя	Наличие на камере омывателя	1 — да, 0 — нет	0
Поддержка стеклоочистителя	Наличие на камере омывателя	1 — да, 0 — нет	0
Использовать TCP	Если переключатель включен, то для получения потоков используется протокол TCP	1 — использовать TCP, 0 — использовать UDP	0
RTSP-порт	Номер порта для передачи данных по протоколу RTSP 554	Целое число от 1 до 65535, согласно спецификации	554
HTTP-порт	Номер порта для передачи данных по протоколу HTTP	Целое число от 1 до 65535, согласно спецификации	80
Onvif-порт	Номер порта для передачи данных по протоколу Onvif	Целое число от 1 до 65535, согласно спецификации	80
Набор профилей	Идентификатор набора профилей	Указанный в листе Profiles либо пустой	Пусто

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Набор записей	Ссылка на идентификатор набора записей в листе Recordings	Указанный в листе Recordings либо пустой	Пусто
UUID	Уникальный идентификатор UUID, который записывается в логах работы системы. Может пригодиться при обращении в техподдержку	Согласно спецификации . Если UUID задан и камера с таким UUID уже есть, то её настройки будут обновлены	Будет сгенерирован новый UUID
ECHDID	Числовой идентификатор камеры в ЕЦХД. Если значение задано, то на камере включается [трансляция в ЕЦХД]	Целое число	Пусто
Транслировать в облако	Включение трансляции в облако	1 — вкл, 0 — выкл	0
Теги	Теги, присвоенные камере	Перечисление идентификаторов тегов, присвоенных камере. Разделитель — пробел. Идентификаторы обычных тегов задаются с префиксом # «решётка» (#ptz), а тегов расположения — с префиксом @ «собака» (@main). Идентификатор вложенного тега указывается через точку после идентификатора вышестоящего тега, например: #schedule.night, @main.gate. Тег расположения может быть присвоен только один, обычных тегов — несколько. Теги должны быть указаны на листе Tags	Пусто
Широта	Координаты камеры — широта	Градусы от -90.0 до 90.0 в виде десятичной дроби. Разделитель — точка	Пусто
Долгота	Координаты камеры — долгота	Градусы от -180.0 до 180.0 в виде десятичной дроби. Разделитель - точка	Пусто
Направление	Направление объектива камеры в градусах	Значение от 0 до 359, где 0° — на восток, 90° — на север, 180° — на запад, 270° — на юг	Пусто
План	Идентификатор плана этажа	Текстовая строка	Пусто

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Аудио	Разрешение трансляции аудио	1 — да, 0 — нет	0

Если на листе Cameras хотя бы у одной камеры заполнен столбец «Набор профилей», то в файле импорта обязательно должны быть описания этих наборов в листе Profiles.

Если на листе Cameras хотя бы у одной камеры заполнен столбец «Набор записей», то в файле импорта обязательно должны быть описания этих наборов в листе Recordings.

Если на листе в Cameras задан UUID камеры и камера с таким идентификатором уже существует в базе. В этом случае:

1. Согласно листу Recordings добавляются правила записи по тем профилям камеры, по которым они отсутствуют.
2. По тем профилям, для которых уже существуют правила записи и для которых на листе Recordings найдена соответствующая запись, в существующих правилах записи обновляется глубина хранения и режим записи (включена или выключена).
3. Удаляются правила записи по тем профилям камеры, для которых отсутствует информация на листе Recordings (только в том случае, если на вкладке Cameras для камеры задан Recording set).

Формат листа Profiles

На листе Profiles обязательные столбцы:

- Набор профилей
- Название
- RTSP-url

Если хотя бы один из них не заполнен, строка будет считаться комментарием.

Остальные столбцы заполнять необязательно. Пустые столбцы будут интерпретироваться со значениями по умолчанию.

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Набор профилей	Идентификатор набора профилей	Целое число от 0 до 2 миллиардов	Поле обязательно для заполнения
Название	Название профиля	Строка, только латинские символы, нижнее подчёркивание и дефис, максимальная длина 64 символа	Поле обязательно для заполнения
RTSP-url	URL-путь для получения видеопотока по протоколу RTSP	URL-путь	Поле обязательно для заполнения
Screen-url	URL-путь для получения скриншотов с камеры по протоколу HTTP	URL-путь	Пусто

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Кодек	Название кодека	Строка не чувствительная к регистру, поддерживается только кодек H264	Пусто
Ширина	Ширина потока	Целое число от 64 до 16384	Пусто
Высота	Высота потока	Целое число от 64 до 16384	Пусто
FPS	FPS потока	Целое число от 0 до 1000	Пусто

Формат листа Recordings

На листе Recordings обязательные для заполнения столбцы:

- Набор записей
- Глубина
- Статус
- Ширина и Высота либо Профиль

Если хотя бы один из них не заполнен, вся строка будет считаться комментарием.

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Набор записей	Идентификатор набора записей	Целое число	Поле обязательно для заполнения
Глубина	Глубина хранения архива в днях	Целое или дробное число	Поле обязательно для заполнения
Статус	Статус записи	1 — запись включена, 0 — выключена	Поле обязательно для заполнения
Ширина	Ширина видеопотока (может отсутствовать, если указан Profile)	Целое число от 64 до 16384	Поле обязательно для заполнения, если не заполнено поле Profile
Высота	Высота видеопотока (может отсутствовать, если указан Profile)	Целое число от 64 до 16384	Поле обязательно для заполнения, если не заполнено поле Profile
Профиль	Идентификатор профиля видеопотока (может отсутствовать, если заданы значения Width и Height). Если указан Profile — проверяется его существование у камеры и правило записи создается с этим профилем. Если Profile не указан или у камеры нет такого профиля, а Width и Height не указаны — импорт камеры не производится	Целое число	Поле обязательно для заполнения, если не заполнены Width и Height

Если значение в столбце «Профиль» не указано или потока с таким профилем на камере нет, то при импорте проверяется наличие правил записи потока по значениям ширины и высоты. Если

правило записи для такого потока с таким разрешением уже создано, новое правило при импорте не создаётся.

Формат листа Tags

На листе **Tags** указывается информация о тегах, которые будут добавлены в справочник тегов и расположений. Необходимо заполнить столбцы:

- Идентификатор;
- Название.

Идентификаторы обычных тегов задаются с префиксом # («решётка»), а тегов расположения — с префиксом @ («собака»). Идентификатор вложенного тега указывается через точку после идентификатора вышестоящего тега, например: #schedule.night, @main.gate.

Пример заполнения листа Tags:

Идентификатор	Название
#ptz	Поворотные камеры
#schedule	Работают по расписанию
#schedule.day	Дневные камеры
#schedule.night	Ночные камеры
@main	Главное здание
@main.entrance	Проходная
@main.gate	Ворота

Подключение камер с видеорегистратора

В Insentry потоки добавляются по очереди с каждого канала видеорегистратора. Чтобы добавить потоки с одного канала:

1. Подключите регистратор к локальной сети.
2. Перейдите в раздел **Управление → Устройства → Камеры → Мастер добавления**.
3. Нажмите кнопку **Камеры нет в списке**.
4. Введите название, IP, логин и пароль для доступа к регистратору.
5. Нажмите кнопку **Далее** и выберите, какие камеры добавить.
6. Закройте окно и перейдите в настройки добавленной камеры. Там будут показаны все видеопотоки, импортированные с видеорегистратора. Удалите лишние, оставив потоки нужного вам канала.

Insentry использует потоки с низким и высоким разрешением, чтобы экономить сетевые ресурсы: при проигрывании видео в маленьких слотах просмотра используется поток с низким разрешением, при просмотре на весь экран — поток с высоким разрешением.

Рекомендуем оставить все потоки, относящиеся к нужным каналам.

Настройки
Права
Теги
Архив
Видеоаналитика

Название

Регистратор_1

Описание

...

Модель камеры

ONVIF onvif ptz camera

Параметры подключения

Расположение

Не задано

Модуль аналитики

InSentry.Spot 1

Модуль архива

InSentry.Keep 1

Лицензия: активна

UUID: faa3c21c-bc64-4ec0-89d5-5119b49a0da2

IPC

2022-03-11 14:45:50

Видеопотоки
Добавить поток

1920×1080@fps20, H264

rtsp://[redacted]@172.17.35.155:554/cam/realmonitor?channel=1&subtype=0&unicast=true&proto=Onvif

352×288@fps20, H264

rtsp://[redacted]@172.17.35.155:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

2688×1520@fps20, H264

rtsp://[redacted]@172.17.35.155:554/cam/realmonitor?channel=2&subtype=0&unicast=true&proto=Onvif

704×576@fps20, H264

rtsp://[redacted]@172.17.35.155:554/cam/realmonitor?channel=2&subtype=1&unicast=true&proto=Onvif

Если нужный видеопоток с регистратора не был добавлен:

1. Посмотрите, как должна выглядеть типовая RTSP ссылка на видеопоток вашей модели видеорегистратора.
2. Откройте [настройки видеопотока](#).
3. Измените пути для RTSP и HTTP.
4. Обновите изображение с камеры.
5. Нажмите кнопку **Сохранить**.

Пример оформления RTSP ссылки на видеопоток видеорегистратора Dahua DHI-NVR4208-8P-4KS2/L:

Настройки потока

rtsp://[redacted]@172.17.35.155:554/cam/realmonitor?channel=1&subtype=0&unicast=true&proto=Onvif

URL снимка камеры

http://[redacted]@172.17.35.155:80/onvifsnapshot/media_service/snapshott?channel=1&subtype=0

IPC

2022-03-11 14:48:22

590×236@fps20, H264

Отмена

Сохранить

Отключение камер

При отключении камеры из системы безвозвратно удаляются записи архива и настройки видеоаналитики.

Чтобы отключить камеру:

1. Перейдите в раздел **Управление → Устройства → Камеры**. Будет представлен [список камер](#).
2. Выберите в списке камеру, которую нужно удалить. Чтобы удалить сразу несколько камер, установите галочки слева от названий нужных камер.
3. Нажмите на кнопку удаления . Будет представлено окно подтверждения удаления камеры.
4. Проверьте названия и адреса камер. Если всё верно, продолжите удаление.

Просмотр списка и статуса работы камер

Для просмотра списка камер перейдите в раздел **Управление → Устройства → Камеры**. Будет представлен список камер, подключенных к Insentry.

Камеры						Добавить камеру
Введите ваш запрос						
Включить расширенный поиск						
Название / IP	Вендор / Модель	Потоки	Архив	Детекторы	Лицензия	
☐  AAC 172.17.17.17 PTZ	ONVIF onvif ptz camera	 3				
☐  Camera 1 172.17.17.17 PTZ	ONVIF onvif ptz camera	 4				
☐  Camera 2 172.17.17.17 PTZ	ONVIF onvif ptz camera	 2				
☐  Camera 3 172.17.17.17 PTZ	ONVIF onvif ptz camera	 3				
☐  Camera 4 172.17.17.17 PTZ	ONVIF onvif ptz camera	 4				
☐  Office 172.17.17.17 PTZ	ONVIF onvif ptz camera	 1				

Для каждой камеры указаны параметры:

- **Название/IP** — [название камеры](#), [IP адрес](#), превью изображения сцены, маркеры:
 - PTZ — для поворотных камер;
 - ЕЦХД — если для камеры настроена [трансляция данных в ЕЦХД](#);
- **Вендор/модель** — [вендор](#) и [модель](#) камеры, указанные в настройках;
- **Потоки** — количество и статус работы [видеопотоков](#);
- **Архив** — количество [правил записи архива](#) и статус записи;
- **Детекторы** — количество и статус [детекторов](#);
- **Лицензия** — [информация о лицензиях](#);

-  — активная постоянная лицензия;
-  — временная лицензия истекла, при наведении курсора отображается дата и время истечения лицензии;
-  — временная лицензия активна, при наведении курсора отображается дата и время истечения лицензии.

Чтобы перейти к [настройкам камеры](#), нажмите на название камеры в списке.

Поиск по списку камер

Строка поиска камер работает в двух режимах: обычном и расширенном.

В обычном режиме можно искать камеры по названию или адресу.

В режиме расширенного поиска можно искать камеры по сочетанию нескольких признаков. Это полезно, например, когда нужно найти камеры, отмеченные определённым тегом и расположенные в одном здании.

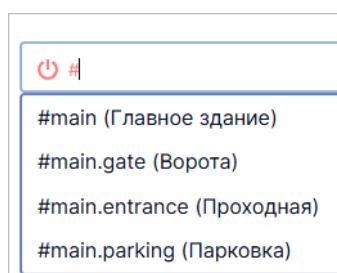
В основе расширенного поиска — логическое выражение, состоящее из параметров и операторов.

Параметры — идентификаторы тегов, заданные в [справочнике тегов и расположений](#).

Операторы — логические операторы связывают между собой значения разных параметров в один запрос. Доступны следующие логические операторы:

- AND — логическое «и»;
- OR — логическое «или»;
- ANY — логическое «любой»;
- NOT — логическое «не»;
- скобки — позволяют настраивать строку поиска подобно математической формуле.

Система выполняет поиск совпадений по справочнику тегов и расположений и отображает контекстный список подсказок. В списке подсказок каждый тег отображается в виде идентификатора и наименования тега, указанного в скобках. Идентификаторы вложенных тегов содержат идентификаторы родительских тегов, указанные через точку в порядке, заданном иерархией справочника тегов. Выбранное обозначение тега автоматически подставляется в поисковую строку.



Обозначения параметров:

Параметр	Обозначение
Тег	#
Расположение	@

Как ввести запрос

1. Переключитесь на расширенный поиск в строке поиска камер.
2. Последовательно выбирайте нужные значения параметров и операторов из раскрывающегося списка.
3. После ввода параметра поставьте пробел и укажите логический оператор AND или OR.
4. Укажите все необходимые значения параметров и логические связи между ними. Если синтаксис запроса верный, значок  в начале поисковой строки будет зелёным. Если он красный, значит, синтаксис неверный. В этом случае введите запрос заново. Чтобы не ошибиться, лучше выбирать все значения из списка, ничего не печатая вручную.
5. После того как запрос сформирован, нажмите кнопку поиска в конце строки , чтобы его выполнить. Будет показан список камер, найденных по введённому запросу.

В таблице ниже приведены примеры поисковых запросов для следующей структуры справочника тегов и расположений:

- теги:
 - tag1:
 - tag11;
 - tag12;
- расположения:
 - location1;
 - location2.

Запрос	Результат
#tag1	Камеры, отмеченные тегом tag1 или любым из вложенных в tag1 тегов
#tag1.tag11	Камеры, отмеченные тегом tag11, вложенным в tag1
@location1	Камеры, отмеченные тегом расположения location1
#tag1 AND @location1	Камеры, расположенные в location1 и отмеченные тегом tag1
#tag11 OR #tag12	Камеры, отмеченные любым из указанных тегов
#tag1 AND NOT #tag12	Камеры, отмеченные тегом tag 1 или вложенными в него тегами, за исключением tag12
ANY	Камеры, которым присвоен любой тег
NOT ANY	Камеры, которым не присвоен ни один тег
NOT @location2	Все камеры, кроме отмеченных тегом расположения location2
(#tag1 AND @location2) AND NOT #tag12	Камеры, расположенные location2 и отмеченные тегом tag1 или вложенными в него, кроме тех, что отмечены тегом tag 12

Индикация работы потоков, архива и видеоаналитики

Проверить параметры работы подключенных камер (fps, битрейта, джиттера, качества потока) за промежуток времени вы можете в отчёте «Доступность камер» (раздел **Отчёты** в главном меню).

В списке камер статусы работы потоков, записи архива и детекторов отображаются в виде цветных индикаторов. Цифра на индикаторе обозначает количество потоков и правил записи. Цвет индикатора отражает текущее состояние работы камеры.

Индикатор	Статус	Потоки	Архив	Детекторы
	Работает штатно	Качество потока более 90% более минуты без ошибок	Запись потока ведётся непрерывно без перезапусков	Детектор работает более 3 минут
	Предупреждение	Качество потока составляет от 50 до 90% либо не выполнены условия работы потока	Не выполнены условия для записи потока либо за последние 3 минуты запись перезапускалась нештатно	Не выполнены условия для запуска детектора либо за последние 3 минуты детектор перезапустился
	Неактивно	Нет информации о потоке	Нет активного правила записи для потока	Детектор настроен, но остановлен
	Проблемы/ошибки	Качество потока менее 50% либо есть ошибки доступа к камере или потоку	Запись архива перезапускается или есть ошибки	Детектор перезапускается
	Критическая проблема	Служба Cast недоступна	Служба Кеер недоступна	Служба Spot недоступна

Для просмотра деталей, наведите курсор на индикатор в соответствующем столбце.

Информация во всплывающих подсказках:

- о потоках:
 - разрешение потока;
 - кадровая частота;
 - стандарт кодека;
 - статус;
 - битрейт (мегабит/с);
 - качество;
 - джиттер;
- о детекторах:
 - название детектора;
 - время работы;
 - среднее время работы;
 - количество перезапусков;
- об архиве:
 - разрешение потока;
 - кадровая частота;
 - стандарт кодека;
 - хранилище;
 - длительность записи;
 - средняя длительность записи;
 - количество перезапусков;
 - статус.

Настройка камер

Для перехода к настройке камеры, перейдите в раздел **Управление → Устройства → Камеры** и нажмите на строку с описанием камеры в [списке камер](#). Будет представлен раздел **Настройки камеры**, состоящий из подразделов:

- **Настройки** — общие параметры камеры: название, модель, IP-адрес, параметры видеопотоков и пр.;
- **Права** — [настройка прав доступа пользователей к управлению камерой и просмотру видеопотоков](#);
- **Теги** — [присвоение камере тегов](#);
- **Архив** — [включение/отключение записи архива](#);
- **Видеоаналитика** — [настройка видеоаналитики](#).
- **Связанные объекты** — [настройка связи с другими устройствами](#), информация с которых может быть полезна при обработке событий, полученных с выбранной камеры.

При переходе в раздел настроек камеры, первой представлена вкладка **Настройки**.

Камеры > 1

Настройки | Права | Теги | Архив | Видеоаналитика | Связанные объекты

Название 1	Модель камеры ONVIF onvif ptz camera	
Описание ...	Параметры подключения 172.17.17.17	
Расположение	Используемые модули Spot 1, Keep 1	
Координаты 5.44102, -5.80078, Графический план	Лицензия: активна UUID: a1d06869-faf4-4372-9333-a1d068694372	

Видеопотоки Добавить поток

	1920×1080@fps25, H264 rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif
	704×576@fps25, H264 rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif
	704×576@fps25, H264 rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

☐ Разрешить трансляцию звука
 ☒ Получать потоки по TCP
 ☐ Транслировать в Insentry.Cloud
 ☐ Транслировать в ЕЦХД
 Настроить

Параметры камеры

Параметры камеры представлены в верхней части экрана, справа расположен скриншот изображения камеры, полученный по протоколу ONVIF.

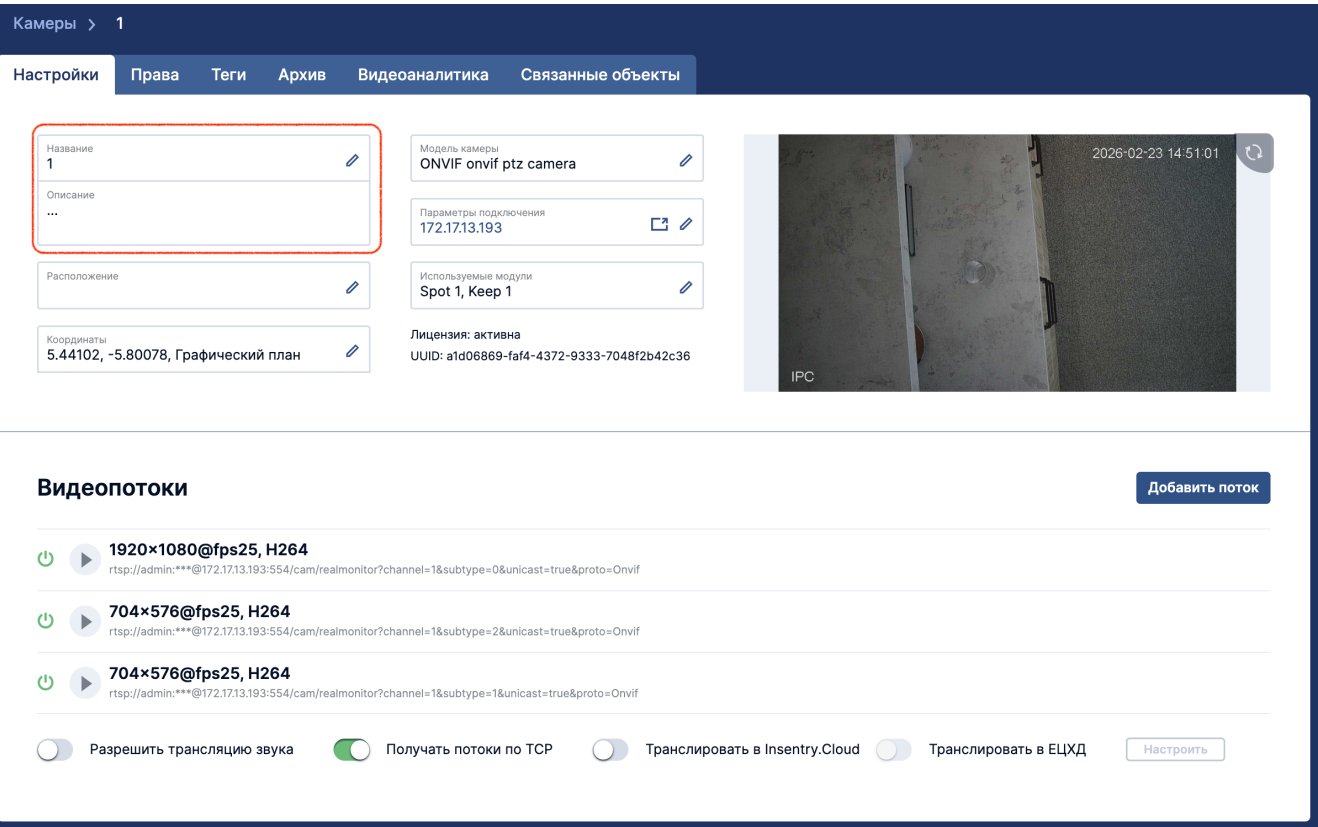
Описание полей приведено в таблице. Ссылки ведут на страницы, посвящённые редактированию соответствующих параметров камеры.

Параметр	Описание	Формат	Можно редактировать
Название	Название камеры в системе	Текстовое поле длиной от 1 до 250 символов. Допустимы символы кириллицы, все печатные символы ASCII	✓
Описание	Описание камеры (свободный текст)	Текстовое поле длиной от 0 до 250 символов. Допустимы символы кириллицы, все печатные символы ASCII	✓
Модель камеры	Вендор и модель камеры	Выбор из списка	✓
Параметры подключения	IP адрес, логин и пароль для доступа к камере, порты подключения	IP — IPv4 адрес или DNS-имя, логин и пароль — текст длиной от 1 до 50 символов (допустимы все печатные символы ASCII), порты — целое число от 1 до 65535, согласно спецификации	✓
Расположение	Здесь можно указать расположение камеры на карте. Список тегов настраивается в справочнике тегов и расположений в разделе Управление → Справочники → Теги и расположения камер	Выбор из справочника	✓
Координаты	Координаты расположения камеры. Используются для отображения расположения камер на карте объекта. В базовой версии системы поле не редактируется и не заполняется	Широта и долгота в градусах. Широта — от -90.0 до 90.0. Долгота — от -180.0 до 180.0. Разделитель дроби — точка	✓
Модуль архива	При использовании расширенной версии системы возможно выбрать расположение модуля архивации — Кеер. В базовой версии системы поле заполнено в соответствии с параметрами раздела Модули и не редактируется	В зависимости от версии, поле заполняется автоматически в соответствии с параметрами раздела Модули либо доступен выбор из списка	✗
Модуль аналитики	При использовании расширенной версии системы возможно выбрать расположение модуля видеоаналитики — Spot. В базовой версии системы поле заполнено в соответствии с параметрами раздела Модули и не редактируется	В зависимости от версии, поле заполняется автоматически в соответствии с параметрами раздела Модули либо доступен выбор из списка	✗
Статус лицензии	Статус используемой лицензии Insentry	—	✗

Параметр	Описание	Формат	Можно редактировать
UUID	Уникальный идентификатор UUID, который записывается в логах работы системы. Может пригодиться при обращении в службу технической поддержки	Согласно спецификации	

Название и описание камеры

Перейдите в раздел **Управление → Устройства → Камеры** и нажмите на строку камеры в списке. Будут открыты настройки камеры.



Нажмите кнопку в поле **Название** и укажите новое название и/или описание камеры. Формат полей: длина до 250 символов, допустимы символы кириллицы и все [печатные символы ASCII](#).
Нажмите кнопку **Сохранить**.

Вендор и модель камеры

Перейдите в раздел **Управление → Устройства → Камеры** и нажмите на строку камеры в списке. Будут открыты настройки камеры.

Камеры > 1

Настройки Права Теги Архив Видеоаналитика Связанные объекты

Название
1

Описание
...

Расположение

Координаты
5.44102, -5.80078, Графический план

Модель камеры
ONVIF onvif ptz camera

Параметры подключения
172.17.17.17

Используемые модули
Spot 1, Keep 1

Лицензия: активна
UUID: a1d06869-faf4-4372-9333-a1d068694372

2026-02-23 14:51:01

IPC

Видеопотоки Добавить поток

- 1920×1080@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif
- 704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif
- 704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

☐ Разрешить трансляцию звука
 ☒ Получать потоки по TCP
 ☐ Транслировать в Insentry.Cloud
 ☐ Транслировать в ЕЦХД
 Настроить

Нажмите кнопку  в поле **Вендор и модель** и укажите новые значения.

В списке моделей представлены модели для выбранного производителя камеры. Если нужной модели нет в списке, проверьте, что в поле **Вендор** указан верный производитель или выберите значение **Other model**.

Чтобы использовать некоторые функции PTZ при управлении поворотными камерами (стеклоочиститель, омыватель и т.д.), здесь обязательно должна быть указана модель камеры, поддерживающая указанные функции.

Модель камеры ✕

Вендор
Hikvision

Модель камеры
Other PTZ-model

Отмена Сохранить

Нажмите кнопку **Сохранить**.

Параметры подключения

Параметры подключения камеры — это её IP адрес, порты, логин и пароль для доступа.

Логин и пароль доступа к камере указываются на этапе [добавления камеры](#) в систему и обеспечивают доступ к работе с видеопотоком камеры. Если логин или пароль уже добавленной камеры был изменён, то нужно указать новые данные в системе.

Редактировать эти параметры можно в настройках камеры (**Управление → Устройства → Камеры** клик по строке с описанием камеры → вкладка **Настройки**), поле **Параметры подключения**.

Камеры > 1

Настройки | Права | Теги | Архив | Видеоаналитика | Связанные объекты

Название: 1

Описание: ...

Расположение:

Координаты: 5.44102, -5.80078, Графический план

Модель камеры: ONVIF onvif ptz camera

Параметры подключения: 172.17.17.17

Используемые модули: Spot 1, Keep 1

Лицензия: активна
UUID: a1d06869-faf4-4372-9333-a1d068694372

2026-02-23 14:51:01

IPC

Видеопотоки Добавить поток

1920×1080@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

☐ Разрешить трансляцию звука ☒ Получать потоки по TCP ☐ Транслировать в Insentry.Cloud ☐ Транслировать в ЕЦХД Настроить

Нажмите кнопку  в поле **Параметры подключения** и укажите новые значения.

Нажмите , чтобы открыть в новой вкладке браузера панель управления камерой.

Форматы значений:

Параметр	Описание	Формат
----------	----------	--------

IP Адрес камеры IPv4 адрес или DNS-имя

Логин и пароль Логин и пароль для доступа к камере Текст длиной от 1 до 50 символов (допустимы все [печатные символы ASCII](#)) RTSP порт Номер порта для передачи данных по протоколу RTSP (по умолчанию — 554) Целое число от 1 до 65535, согласно [спецификации](#)

HTTP порт Номер порта для передачи данных по протоколу HTTP (по умолчанию — 80) Целое число от 1 до 65535, согласно [спецификации](#)

Onvif порт Номер порта для передачи данных по протоколу Onvif (по умолчанию — 80) Целое число от 1 до 65535, согласно [спецификации](#)

Параметры подключения

IP адрес*
192.168.224.7

HTTP
80

RTSP*
554

Onvif порт

Логин
admin

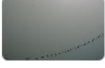
Пароль
.....

Отмена

Сохранить

Проверка доступности камеры

Чтобы убедиться, что камера доступна и данные передаются корректно, вернитесь в раздел **Камеры** и проверьте статус потоков камеры в [списке камер](#). Цифры в поле **Потоки** записаны в формате *Количество активных потоков/Общее количество потоков*. Зелёный цвет индикатора статуса означает, что всё в порядке. Для просмотра деталей по каждому потоку, наведите курсор мыши на значок статуса.

Камеры			
Название / IP	Вендор / Модель	Потоки	Архив
 Reception New Back 192.168.224.70	ONVIF onvif camera	2	1
 Reception New Front 192.168.224.65	ONVIF onvif camera	2	
 Reception Old 192.168.224.59	ONVIF onvif camera	2	1

1920×1080@25, H264
Local storage
Длительность: 2 часа
Средняя длительность: 18 часов
Перезапусков: 12
Статус: Ведётся запись

Чтобы проверить работу ONVIF, перезагрузите кадр в верхней части экрана. Большинство камер будут корректно отображать кадр, если корректно указаны значения модели, вендора камеры и данные для доступа к ней — логин и пароль.

Даже если кадр не отображается, могут быть получены корректные данные видеопотоков, так как потоки и скриншот получены по разным протоколам и не связаны друг с другом.

Расположение камеры

Расположение камеры, как правило, отражает место, где камера находится в здании, или то, в каком здании камера расположена — например, «1 этаж» или «Главное здание». Список мест задаётся в [справочнике тегов и расположений](#).

Чтобы присвоить камере расположение:

1. Перейдите в настройки камеры.
2. Нажмите кнопку **Редактировать**  в поле **Расположение**. Будет представлено окно выбора расположения камеры.
3. Выберите нужный тег из списка тегов расположения.
4. Нажмите кнопку **Сохранить**.

Камеры > 1

Настройки
Права
Теги
Архив
Видеоаналитика
Связанные объекты

Название
1

Описание
...

Расположение

Координаты
5.44102, -5.80078, Графический план

Модель камеры
ONVIF onvif ptz camera

Параметры подключения
172.17.17.17

Используемые модули
Spot 1, Keep 1

Лицензия: активна
UUID: a1d06869-faf4-4372-9333-a1d068694372

2026-02-23 14:51:01

IPC

Видеопотоки
Добавить поток

1920×1080@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

Разрешить трансляцию звука

Получать потоки по TCP

Транслировать в Insentry.Cloud

Транслировать в ЕЦХД

Настроить

Задать расположение

+ Главное здание

Филиал Пушкинская
Филиал Сокольники

Проходная

Ворота

Крыша

Сбросить

Сохранить

Координаты камеры

Географические координаты камеры задают расположение камеры на карте.

Перейдите в раздел **Управление → Устройства → Камеры** и нажмите на строку камеры в списке. Будут открыты настройки камеры.

Камеры > 1

Настройки
Права
Теги
Архив
Видеоаналитика
Связанные объекты

Название
1

Описание
...

Расположение

Координаты
5.44102, -5.80078, Графический план

Модель камеры
ONVIF onvif ptz camera

Параметры подключения
172.17.17.17

Используемые модули
Spot 1, Keep 1

Лицензия: активна
UUID: a1d06869-faf4-4372-9333-a1d068694372

2026-02-23 14:51:01

IPC

Видеопотоки
Добавить поток

1920×1080@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

☐ Разрешить трансляцию звука
☒ Получать потоки по TCP
☐ Транслировать в Insentry.Cloud
☐ Транслировать в ЕЦХД

Настроить

Нажмите кнопку  в поле **Координаты** и укажите значения координат в градусах в виде десятичной дроби через точку, например: 55.824547, 37.365913.

Скопировать координаты можно из онлайн карт. В картах Яндекс и Гугл сначала указана широта, затем долгота.

Координаты камеры

Широта*

Долгота*

Этаж
Не выбрано

Направление объектива камеры в градусах
0° — на восток, 90° — на север, 180° — на запад, 270° — на юг

Отмена

Сохранить

Изменить расположение камеры на карте можно в разделе **Управление** → **Карты** → **Объекты**.

Настройка видеопотоков

Просмотр списка потоков

Перейдите в раздел **Управление** → **Устройства** → **Камеры** клик по строке с описанием камеры (**Настройки камеры**) → вкладка **Настройки**. В нижней части экрана представлен блок управления видеопотоками.

The screenshot shows the 'Камеры' (Cameras) section with a sub-tab 'Настройки' (Settings). The interface includes fields for camera name, description, location, coordinates, model, connection parameters, and modules. A live video feed is displayed on the right. Below the settings, the 'Видеопотоки' (Streams) section is highlighted with a red box. It contains a list of three streams, each with a play button icon, resolution, frame rate, and codec. Below the list are four toggle switches for audio streaming, TCP streams, Insentry.Cloud transcoding, and ECU transcoding, along with a 'Настроить' (Configure) button.

Название	Описание	Расположение	Координаты	Модель камеры	Параметры подключения	Используемые модули	Лицензия
1	...		5.44102, -5.80078, Графический план	ONVIF onvif ptz camera	172.17.17.17	Spot 1, Keep 1	активна UUID: a1d06869-faf4-4372-9333-a1d068694372

Видеопотоки

- 1920×1080@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif
- 704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif
- 704×576@fps25, H264
rtsp://admin:***@172.17.13.13:554/cam/realmonitor?channel=1&subtype=1&unicast=true&proto=Onvif

☐ Разрешить трансляцию звука
 ☒ Получать потоки по TCP
 ☐ Транслировать в Insentry.Cloud
 ☐ Транслировать в ЕЦХД
 Настроить

В блоке **Видеопотоки** представлен список настроенных видеопотоков камеры и проигрыватель для воспроизведения видео.

Потоки передаются по протоколу RTSP. Для каждого потока указано его разрешение и URL-адрес.

Для снижения нагрузки на процессор и экономии сетевых ресурсов, при наличии на камере потоков с более низким разрешением, чем HD, для просмотра потока на многослотовой раскладке будет выбираться поток, наиболее близкий к площади видеоокна. Если таких потоков нет или не указаны параметры потока, будет выбран поток наилучшего качества. Для просмотра потока в полноэкранном режиме используется HD-поток или поток наилучшего качества.

This close-up screenshot shows the 'Видеопотоки' (Streams) section. It features a list of two streams with their respective resolutions, frame rates, and codecs. Each stream entry has a play button icon and a close button (X). Below the list are three toggle switches for TCP streams, Insentry.Cloud transcoding, and ECU transcoding, along with a 'Настроить' (Configure) button.

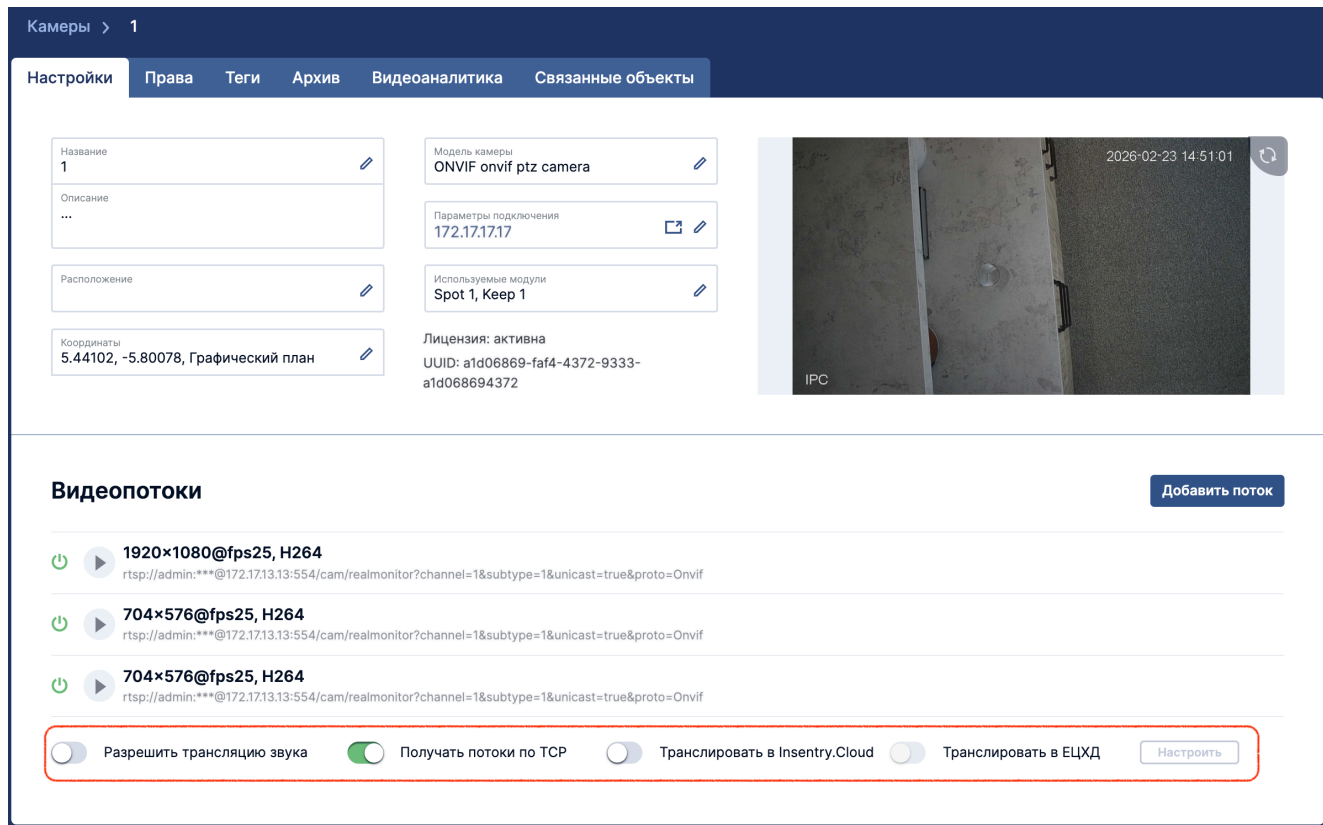
Разрешение	Частота кадров	Кодировщик	URL-адрес
1920×1080	fps25	H264	rtsp://admin:***@172.17.13.209:554/Streaming/Channels/01/
704×576	fps22	H264	rtsp://admin:***@172.17.13.209:554/Streaming/Channels/02/

☐ Получать потоки по TCP
 ☐ Транслировать в Insentry.Cloud
 ☐ Транслировать в ЕЦХД
 Настроить

При наведении курсора на строку с описанием потока, доступны действия с потоком:

-  — воспроизвести поток в окне плеера,
-  — редактировать URL потока,
-  — удалить поток.

Настройки видеопотоков



Разрешить трансляцию звука — включите, чтобы разрешить транслировать звук с камеры. Работает для камер, поддерживающих аудиокодеки AAC или G.711.

Получать потоки по TCP — если настройка выключена, то используется протокол UDP (по умолчанию). Настройка действует на уровне камеры и распространяется на все получаемые с неё потоки.

Переключатель **Транслировать в Insentry.Cloud** позволяет передавать в облачное хранилище данные с камеры для просмотра видеопотока в режиме реального времени и записи архива.

Переключатель **Транслировать в ЕЦХД** позволяет [выгружать данные для ЕЦХД](#).

Проверка доступности потока

Проверить доступность потока камеры по URL можно в медиаплеере с функцией проверки потока по URL, например, [VLC](#). Если поток доступен там, то и в системе тоже будет доступен.

Чтобы проверить доступность потока в системе, нажмите кнопку  на области просмотра потока при его добавлении или справа от списка потоков. Если изображение обновляется — значит поток доступен.

Добавление потока

Чтобы добавить новый поток камеры, нажмите **Добавить поток** и укажите его URL-путь и параметры (если есть).

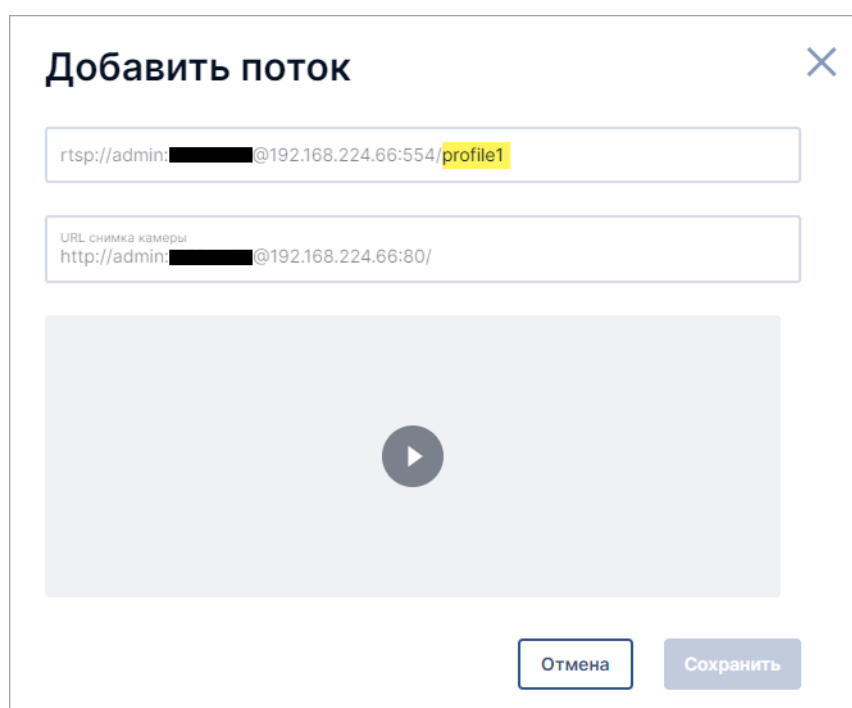
Потоки должны быть предварительно настроены в конфигурации камеры.

Часть URL-локатора от начала до порта подставляется из [параметров камеры](#) и недоступна для редактирования.

URL-путь и параметры потока согласно структуре URL следует указывать в конце:

`rtsp://[логин]:[пароль]@[IP адрес или hostname]:[порт]/[путь]?[параметры]` ,
например: `rtsp://login:password@192.168.0.1:554/profile1` .

В поле **URL снимка камеры** можно указать путь для получения снимка потока. Снимок будет отображаться в верхней части окна настроек камеры. Это поле опциональное: если путь не задан, то возможности получить снимок созданного потока не будет.



Нажмите  на области просмотра, чтобы проверить доступность видео по указанному адресу. Если воспроизведение началось — значит поток доступен.

Переключатель **Использовать только для видеоаналитики** позволяет добавить поток, который будет использоваться только для видеоаналитики. Такой поток будет недоступен для трансляции в ЕЦХД, Insentry.Cloud или для работы с видеоархивом. При добавлении потока, используемого только для видеоаналитики, система проверяет, соответствуют ли параметры потока [рекомендуемым](#) для видеоаналитики. Рекомендуемые параметры потока обеспечивают стабильную и качественную работу видеоаналитики. Проверку можно отключить в настройках интерфейса. Вы можете сохранить поток и использовать его для видеоаналитики, даже если он не соответствует рекомендуемым критериям.

Редактирование URL-пути потока

Чтобы отредактировать URL-путь и параметры потока, наведите курсор на строку с описанием потока, нажмите кнопку редактирования  и укажите новый путь и параметры аналогично тому, как это делается при добавлении потока.

Видеопотоки

Добавить поток

1920×1080@fps25, H264 rtsp://admin:***@172.17.13.209:554/Streaming/Channels/01/	▶ ✎ ✕
704×576@fps22, H264 rtsp://admin:***@172.17.13.209:554/Streaming/Channels/02/	

☐ Получать потоки по TCP
 ☐ Транслировать в Inentry.Cloud
 ☐ Транслировать в ЕЦХД

Настроить

Если в редактируемой части URL-локатора потока указаны неверные данные, измените соответствующие параметры в [настройках камеры](#).

Замена недоступного потока

Если поток стал недоступен, например, из-за изменения конфигурации профилей на камере или прошивки камеры, то в списке потоков он выделяется красным цветом.

Нажмите на недоступный поток, чтобы заменить его на другой.

Заменить поток

✕

Поток 640×480@10fps, H264 недоступен на камере. Выберите, какой поток использовать вместо него для видеоаналитики и записи архива.

1920x1080@25fps, H264

rtsp://admin:***@11.71.0.243:554/Streaming/Channels/02/

720x480@30fps, H264

rtsp://admin:***@11.71.0.243:554/Streaming/Channels/Streaming/Channels/Streaming/Channels/02/

Отмена

Готово

Настройка безопасности камеры. Права доступа

Права доступа настраиваются двумя способами:

1. *на уровне камеры* — определением в настройках камеры, кому из пользователей разрешён доступ к операциям с камерой;
2. *на уровне пользователя* — определением в настройках учётной записи, какие разрешения действуют для учётной записи.

Для настройки на уровне камеры, перейдите в раздел **Управление → Устройства → Камеры**, выберите камеру в списке. Откроются настройки камеры. Перейдите на вкладку **Права**.

Для настройки на уровне пользователя, перейдите в настройки учётной записи в разделе **Управление → Пользователи** и откройте вкладку **Камеры**.

В каждом случае возможно задать разрешение на выполнение следующих операций:

- доступ к просмотру потока камеры в реальном времени (см. *Руководство пользователя, раздел Просмотр живого видео и архива*);
- просмотр архива (см. *Руководство пользователя, раздел Просмотр видеоархива*);
- экспорт архива (см. *Руководство пользователя, раздел Экспорт архива*);
- формирование и просмотр отчётов;
- управление поворотными камерами (PTZ);
- настройки камер.

Разрешение доступа к разделам **Наблюдение, Отчеты, Настройки** определяет:

1. видимость разделов главного меню — пользователю доступны соответствующие разделы главного меню системы, если доступ к ним разрешён на уровне хотя бы одной камеры. В противном случае раздел не отображается;
2. отображение камеры в [списке камер](#) — пользователю показаны только те камеры, к которым ему разрешён доступ хотя бы в одном из этих разделов;
3. отображение в списке событий — пользователю показаны события только с тех камер, к которым ему разрешён доступ хотя бы в одном из этих разделов.

Разрешение операции **Экспорт** определяет доступ к разделу **Экспорт** и возможность экспорта архива камеры в разделе **Просмотр**.

Разрешение доступа к **PTZ** даёт возможность управлять положением камеры, дворниками, омывателем на странице просмотра видео (см. *Руководство пользователя, раздел Просмотр живого видео и архива*) в разделе **Просмотр**.

Права имеют вложенную структуру. Чтобы предоставить доступ к разделу PTZ, необходимо сперва предоставить доступ к наблюдению (просмотр потока камер (см. *Руководство пользователя, раздел Просмотр живого видео и архива*)), а чтобы разрешить экспорт архива (см. *Руководство пользователя, раздел Экспорт архива*), необходимо сперва разрешить работу с архивом.

Присвоение камере тегов

Теги используются для обозначения свойств камер. Список тегов настраивается в [справочнике тегов и расположений](#) в разделе **Управление → Справочники → Теги и расположения камер**.

Чтобы присвоить теги камере:

1. Откройте настройки камеры.
2. Перейдите на вкладку **Теги**. Будет представлен список присвоенных камере тегов.
3. Нажмите кнопку **Добавить**. Откроется модальное окно со списком тегов. Теги имеют иерархическую структуру. Для просмотра вложенных тегов нажмите кнопку «плюс» слева от названия родительского тега.
4. Отметьте требуемый тег.
5. Нажмите кнопку **Сохранить**. Тег будет присвоен камере.
6. Если требуется присвоить камере несколько тегов, повторите операцию, начиная с п. 3.

Выбрать теги

Поворотные камеры

—

Работают по расписанию

Ночные камеры

Дневные камеры

+

Видеоаналитика

Сбросить

Сохранить

Настройка записи в архив

Архив записывается в хранилище на локальном компьютере или сетевой папке с определённой глубиной записи. Параметры записи определяются в правиле записи. Для камеры может быть создано несколько правил записи с различными параметрами.

Чтобы включить запись архива:

1. Перейдите в раздел **Управление → Устройства → Камеры** и кликните на строку камеры в списке. Будут открыты настройки камеры.
2. Перейдите на вкладку **Архив**.
3. Нажмите кнопку **Добавить правило записи**.

Правило записи — это настройки того, когда и какой поток с камеры будет записан в архив, а также где будут храниться эти записи.

Один и тот же поток не может записываться в одно хранилище дважды, поэтому нельзя создать больше одного правила записи потока в одно хранилище.

Новое правило записи

Хранилище

Local storage

Поток

1920×1080@0fps, H264

Лимит (суток)

10

Включить запись

Отмена

Сохранить

4. Укажите данные:

- **Хранилище** — место на жёстком диске или в сетевой папке, где будут расположены записи. Расположение папок хранилища можно проверить [в настройках модуля Кеер](#).
- **Поток** — какой из потоков камеры будет записан. Если камера поддерживает несколько видеопотоков, то по умолчанию выбран поток с наилучшим качеством. Список потоков камеры можно просмотреть в блоке **Видеопотоки** на вкладке **Основные**.
- **Лимит (суток)** — количество суток, прошедших от текущего момента, в течение которых архив будет записываться в хранилище. Старые записи перезаписываются новыми, например, если указан лимит двое суток, то в файле архива будет запись за последние двое суток;
- **Включить запись** — можно сразу включить запись потока, а можно создать правило записи, не включая запись.

5. Нажмите кнопку **Сохранить**. Откроется список правил записи. Чтобы начать записывать ещё один поток, нажмите **Добавить**. Кнопка активна только если у камеры есть потоки, для которых можно настроить запись в архив.

Правило записи					Добавить	
Хранилище	Лимит (суток)	Запись	Статус	Условия записи		
Local storage 1920×1080@0fps, H264	10	☒ Включена		Всегда +		

6. По умолчанию запись ведётся в режиме 24/7. Вы можете включить запись по условию и настроить запись по определённому расписанию или по срабатыванию детектора/датчика. Чтобы добавить условие записи, нажмите на плюс в столбце **Условия записи**.

В режиме записи по событию доступна настройка предзаписи и постзаписи — количества секунд видео, которое будет храниться в буфере на случай возникновения события и запишется в событие при его возникновении. Если параметры не заполнены, то предзапись и постзапись не ведётся.

Новое условие записи

Движение в области кадра

×

Предзапись

Нет

▼

Постзапись

5 секунд

▼

Сохранить

1. Включите переключатель в столбце **Запись**. Запись начнётся, в поле **Статус** будет отображён статус записи.

Связанные объекты

Связанные объекты — устройства, информация с которых может быть полезна при обработке тревог, полученных с камеры. Связанные объекты добавляются в настройках камеры в разделе **Управление → Устройства → Камеры → Настройки камеры → Связанные объекты**.

Настройки	Права	Теги	Архив	Видеоаналитика	Связанные объекты			
Связанные объекты						Добавить		
Тип	Название	IP адрес	Вендор / Модель	Расположение	Связь	На карте	Описание	
Камера		1	onvif onvifptzcamera		↓			
Камера		Холл	onvif onvifptzcamera		↑	✓		

Связи имеют направление. Когда в настройках устройства А добавляется связь с устройством В , на странице устройства В автоматически добавляется связь с устройством А . Такая связь означает, что при возникновении тревоги на устройстве А пользователю будет также предоставляться информация с устройства В.

При создании на устройстве А связи с устройством В, направление связи на устройстве А всегда будет исходящим, а на В — входящим. Если в настройках устройства В также добавить связь с устройством А, связь между ними станет двунаправленной  .

Для добавления связи с устройством:

1. В списке связанных объектов нажмите кнопку **Добавить**.
2. В модальном окне выберите устройство, с которым должна быть установлена исходящая связь. Поддерживается [расширенный поиск устройств](#).
3. Нажмите кнопку **Сохранить**. Выбранное устройство появится в списке связанных объектов.

Для удаления связи с устройством, в списке связанных объектов нажмите на крестик в столбце **Входящая/исходящая связь** и подтвердите удаление связи в модальном окне. Если установлена двунаправленная связь, то при удалении одной связи другая остаётся действующей.

Связанные объекты					
Тип	Название	IP адрес	Вендор / Модель	Расположение	Входящая / исходящая связь
Камера		test 41 172.17.13.233	onvif onvifptzcamera		 
Камера		test 33 172.17.13.221	onvif onvifptzcamera		 
Камера		test 06 172.17.13.33	onvif onvifptzcamera		   

Настройка видеоаналитики

Для настройки видеоаналитики требуется установить модуль Spot.

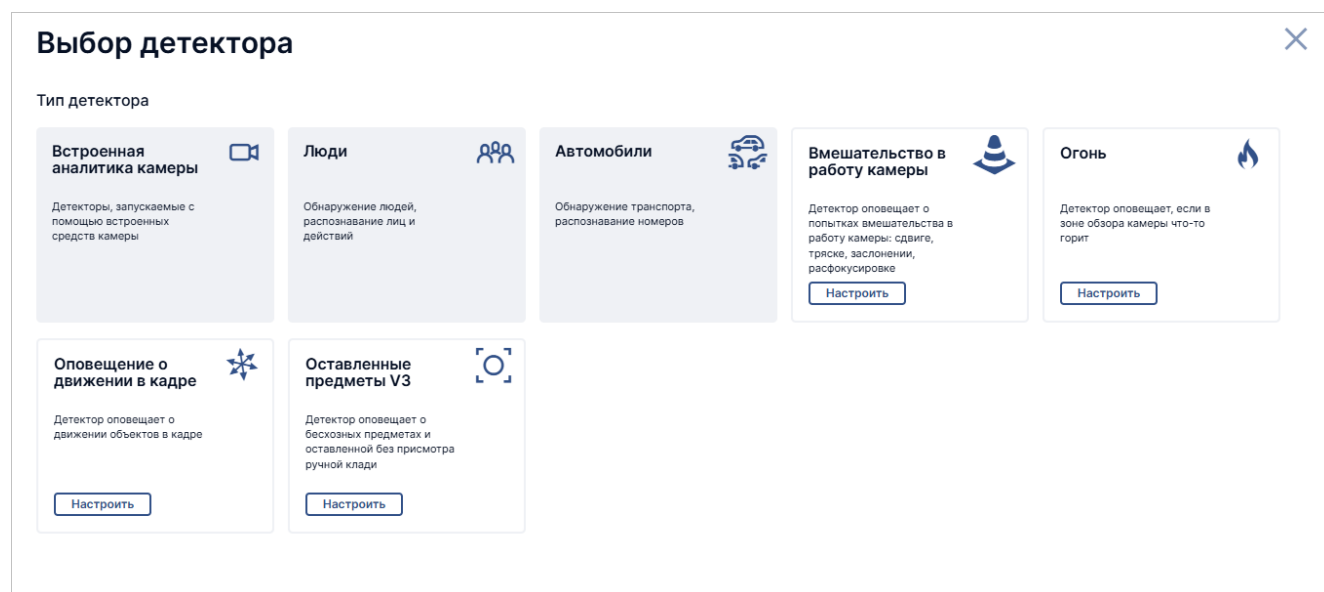
Видеоаналитика позволяет отслеживать наступление определённых событий и анализировать изображение в зоне охвата объектива камеры, чтобы оповестить пользователя о ситуации, требующей внимания. В основе видеоаналитики — настройки детекторов, которые определяют, какие события будут отслеживаться и как Insentry будет реагировать на них. В зависимости от типа детектора, при наступлении отслеживаемого события система реагирует следующим образом:

1. по срабатыванию детекторов, отслеживающих наступление определённого события, система генерирует тревогу и формирует карточку события, которую можно просмотреть в разделе **События**. На таймлайне при видеонаблюдении и просмотре архива (см. *Руководство пользователя, раздел Просмотр живого видео и архива*) появляется метка события;
2. по срабатыванию детекторов, выполняющих аналитические функции, к примеру, подсчёт количества людей, — система анализирует частоту/количество событий и формирует отчёт (см. *Руководство пользователя, раздел Отчёты*).

Внимание! Для корректной работы детекторов необходима видеокарта **Nvidia** не ниже **1050ti**, на **ATI Radeon** детекторы работать не будут.

Добавление нового детектора

Новые детекторы добавляются при помощи мастера:



Детекторы распределены по папкам, чтобы было проще найти нужный. Папки отмечены голубым цветом. Плашки с настройками конечных детекторов — белым.

Просмотр статуса работы детекторов

Перейдите в раздел **Управление → Устройства → Камеры** → клик по строке с описанием камеры (**Настройки камеры**) → вкладка **Видеоаналитика**.

Если ни одного детектора на камере не настроено, то система предложит перейти к настройке. В этом случае нажмите кнопку **Добавить детектор** и настройте сценарий работы хотя бы одного детектора.

Статусы работы настроенных детекторов отображаются в списке детекторов:

Камеры > Gates

Настройки Права Теги Архив Видеоаналитика Связанные объекты

Детекторы Калибровка камеры Добавить

Название	Состояние	Статус	FPS	Запущен	Перезапуски	Среднее время работы	Расписание
Очереди			6.254	11.07.2021 14.52.24	0	около 2 часов	Всегда
Люди в запрещённой зоне			0	11.07.2021 14.53.43	8	0	Всегда
Подсчет людей							Всегда
Пол, возраст, эмоции			3.685	11.07.2021 14.51.57	0	около 2 часов	Всегда
Распознавание гос. номеро...			2.555	11.07.2021 14.48.47	0	около 2 часов	Всегда

Показаны следующие данные:

- название детектора,
- состояние — включен или выключен,
- статус работы,
- FPS,
- дата и время запуска,
- количество перезапусков,
- среднее время работы,
- [расписание](#).

Обозначения статусов работы детекторов:

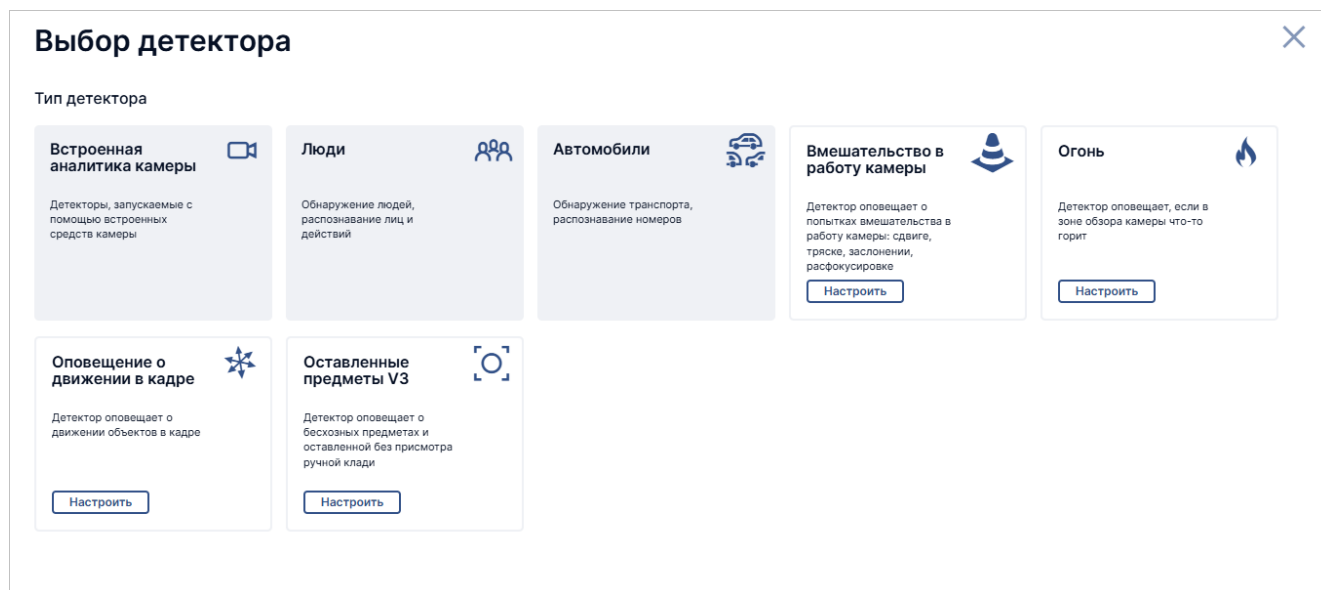
Детектор работает	Детектор не работает	Детектор работает нестабильно
Детектор выключен	Детектор ни разу не был включен	Детектор не может быть включен

Настройка детекторов

Внимание! Для корректной работы детекторов необходима видеокарта **Nvidia**, на **ATI Radeon** детекторы работать не будут.

Видеоаналитика настраивается на уровне камеры в разделе **Управление → Устройства → Камеры → Настройки камеры** (клик по строке с описанием камеры) → вкладка **Видеоаналитика**.

Новые детекторы добавляются при помощи мастера:

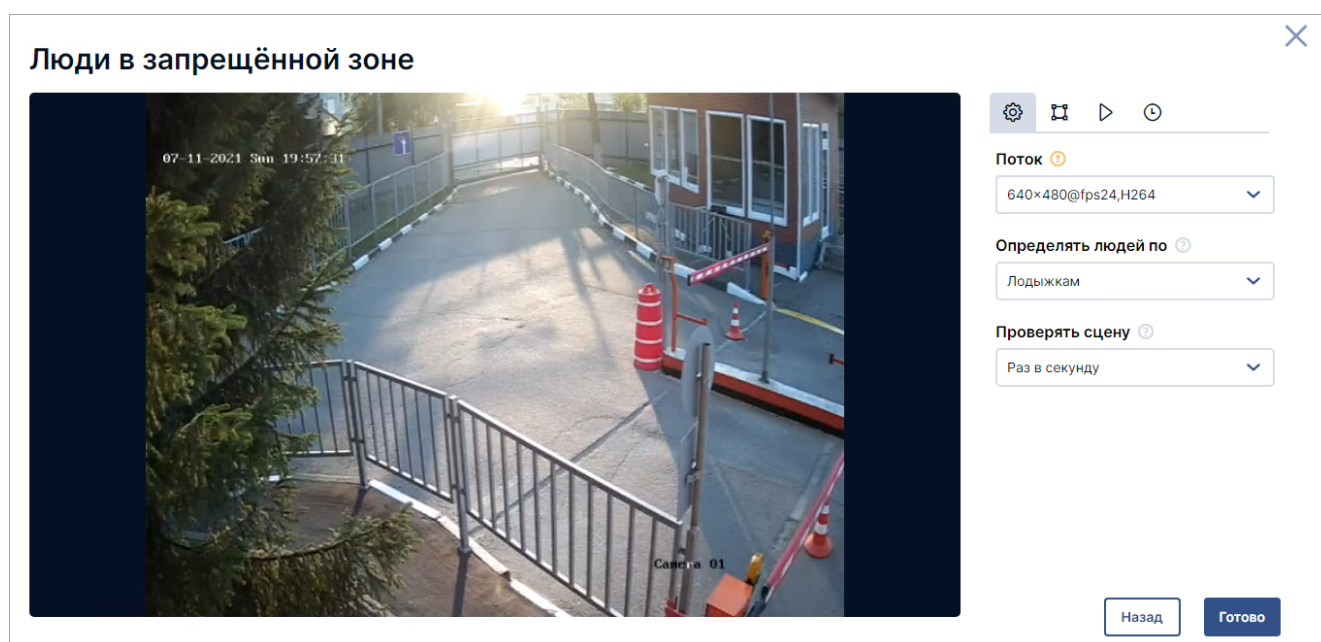


Детекторы распределены по папкам, чтобы было проще найти нужный. Папки отмечены голубым цветом. Плашки с настройками конечных детекторов — белым.

Экран настройки детекторов содержит четыре подраздела:

- — общие настройки;
- — разметка;
- — тестовый запуск работы детектора с текущими настройками;
- — **расписание** работы детектора.

В зависимости от детектора содержимое подразделов различается.

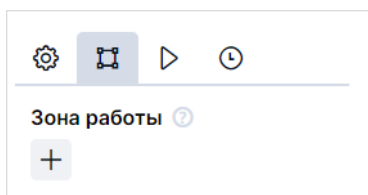


Разметка видеоаналитики

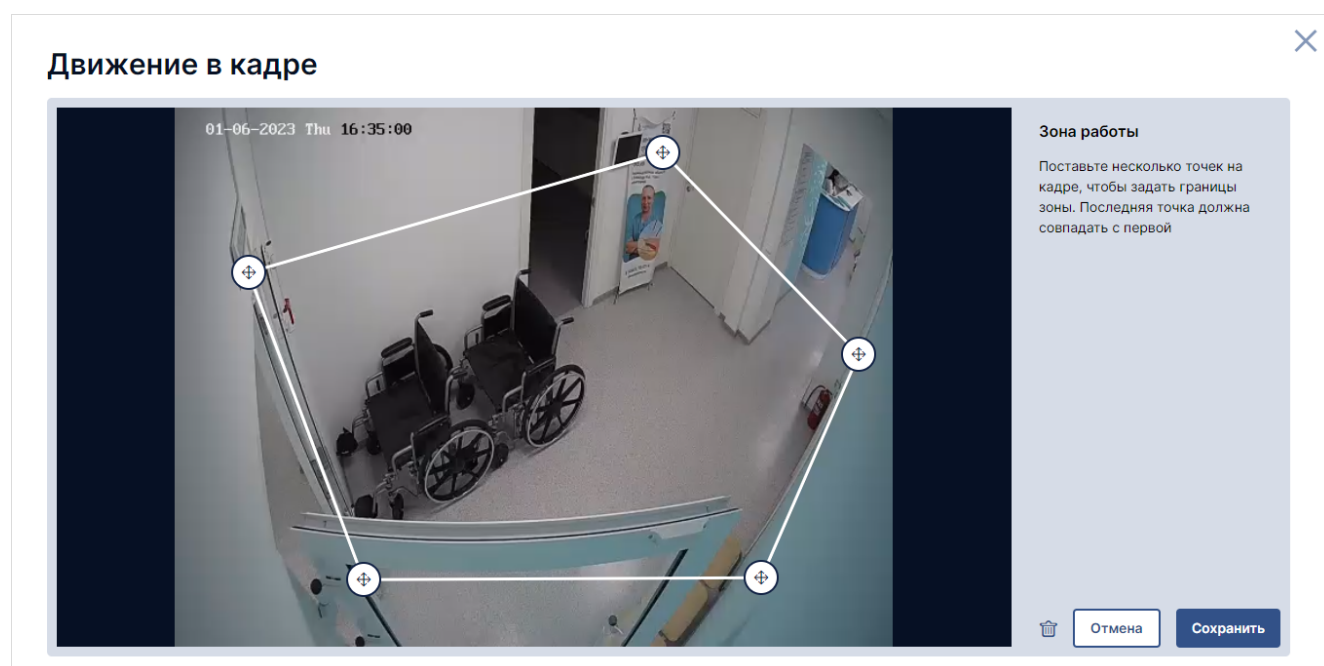
Для настройки некоторых детекторов требуется указать на кадре различные параметры: контрольные линии, границы зон, направление движения. Для примера рассмотрим настройку детектора движения.

Добавление разметки

1. Перейдите к графическим настройкам детектора.



1. Нажмите на плюс (+), чтобы добавить новую зону работы. В окне плеера включится режим редактирования:



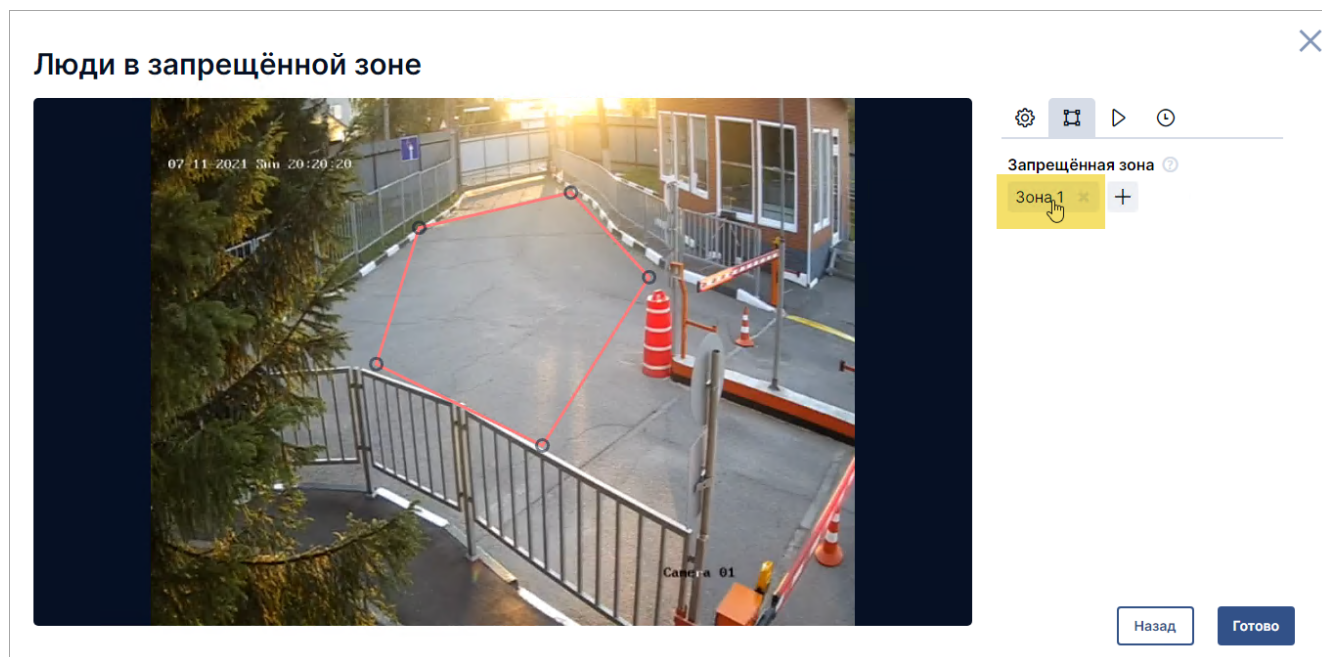
2. Поставьте несколько точек на кадре. Они будут автоматически соединены линиями. В случае настройки других детекторов таким же образом можно расположить на кадре другие графические настройки. Тип и форма графических настроек зависит от типа детектора (овал, линия и т.д.).

Теперь можно двигать установленные ранее точки, чтобы скорректировать границы зоны, перемещая элемент  произвольно по кадру.

Чтобы полностью удалить фигуру и начать заново, нажмите  справа от кадра.

Чтобы сохранить эту зону, нажмите .

Чтобы удалить настроенную зону, кликните на её название. При наведении курсора на название зоны, разметка зоны будет подсвечена на кадре красным цветом, чтобы вы могли проверить зону перед тем как удалить.



Редактирование разметки

Чтобы изменить разметку, нажмите на название разметки в настройках (в нашем случае это **Зона 1**) и измените расположение элементов на кадре.

Чтобы отменить все изменения без сохранения, нажмите . Чтобы сохранить новые настройки, нажмите .

Внимание! При первичной настройке рекомендуется задать все параметры и только после этого включать детектор. В дальнейшем после любых изменений настроек детектора обязательно перезапустите детектор, чтобы изменения вступили в силу.

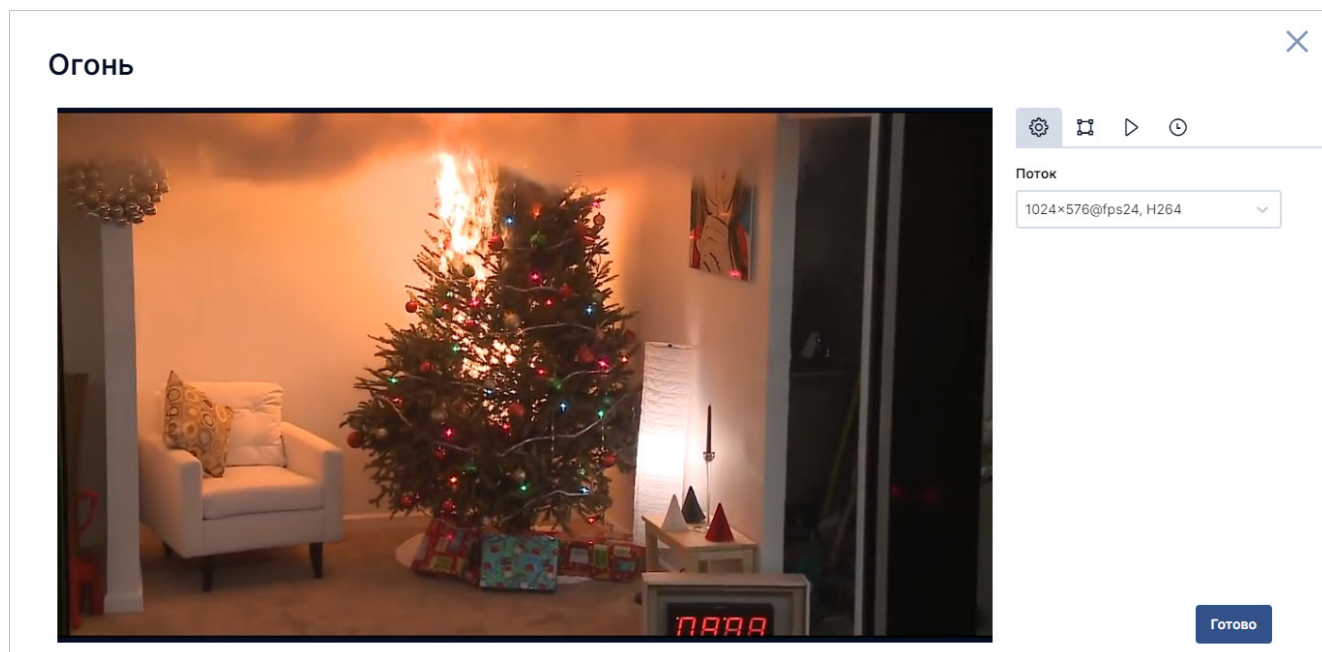
Детектор огня

Детектор отправляет оповещение, если на сцене что-то горит, и отмечает на кадре место, где обнаружен огонь.

Для корректной работы детектора необходима видеокарта Nvidia. На ATI Radeon детектор работать не будет.

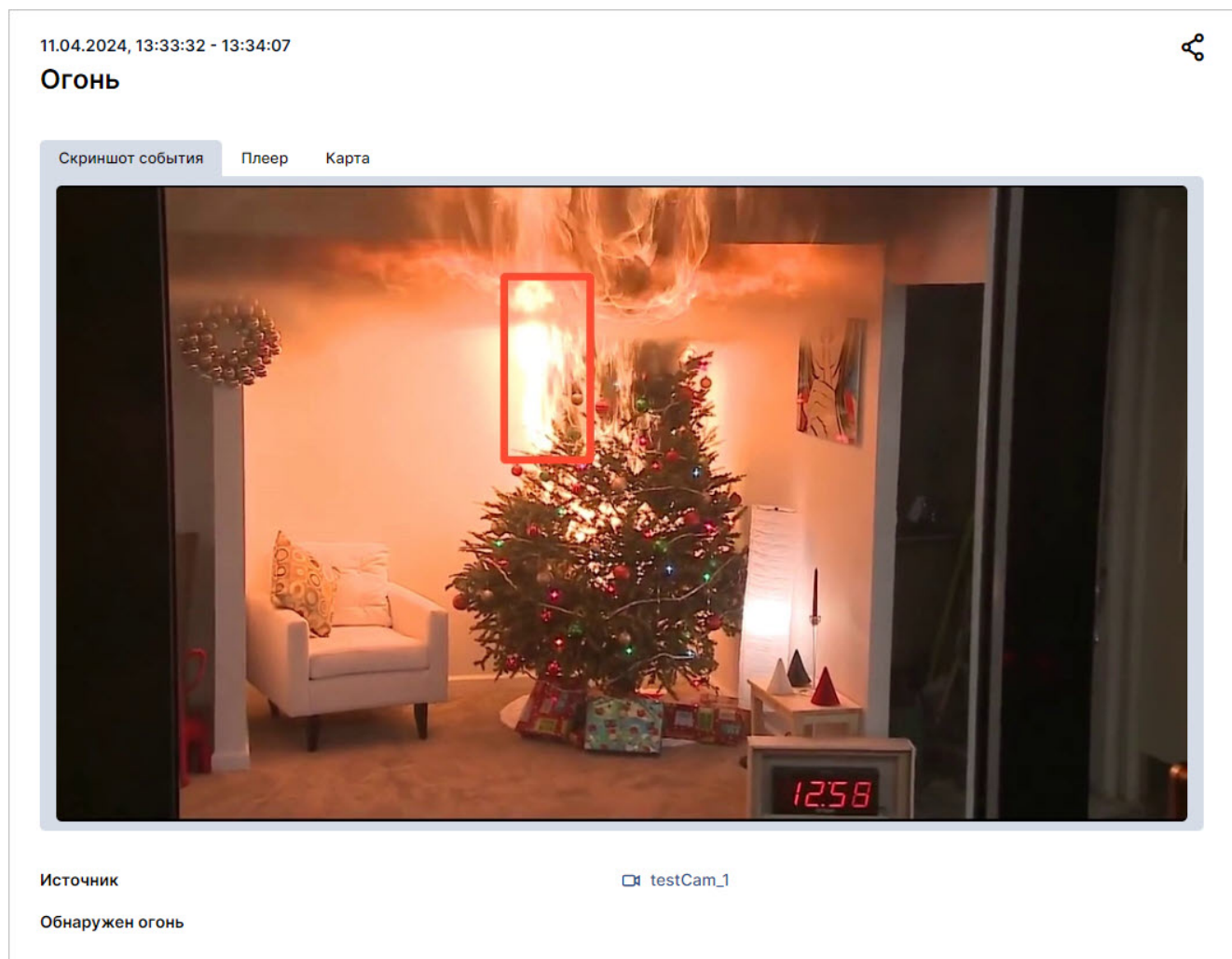
Настройка

Настройка производится в разделе **Управление → Устройства → Камеры → Настройки камеры → Видеоаналитика**.



Параметр	Описание
Поток	Если у камеры несколько потоков, возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками. Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 640×360

Событие:



Вмешательство в работу камеры

Детектор оповещает о попытке вмешательства в работу камеры.

Внимание! Детектор вмешательства в работу камеры является CPU-детектором. Для его работы наличие видеокарты Nvidia не обязательно.

Описание

Детектор отслеживает следующие типы событий:

- заслонение,
- затемнение,
- расфокусировка камеры,
- поворот,
- тряска.

При наступлении одного или нескольких из этих событий детектор генерирует оповещение о вмешательстве в работу камеры.

Условия работы

Модуль детекции расфокусировки, заслонения, затемнения

Режим	Описание
Дневное освещение, неоднотонный фон, стабильная работа канала передачи видеопотока	<u>Заслонение/затемнение:</u> 1. Фиксируются заслонения и непрозрачными, и частично прозрачными предметами. 2. Игнорируются люди на сцене, т.е. до тех пор, пока заслоняющий объект идентифицируется как человек, детектор не срабатывает. 3. Плавное изменение времени суток или освещенности не детектируется как событие. 4. Кратковременное изменение состояния (например, пролетевшая перед камерой птица) не детектируется как событие. <u>Расфокусировка:</u> Детекция срабатывает при неизменной сцене без заслоняющих объектов или с частично прозрачными искажающими изображение объектами, если значительная часть краёв объектов на сцене перестаёт быть хорошо видна
Движение объектов близко от камеры	<u>Заслонение/затемнение:</u> Будет зафиксировано заслонение любым объектом, кроме человека. Примечание: объект исключается из фактора заслонения до тех пор, пока камера идентифицирует его как человека. <u>Расфокусировка:</u> Если на камере нет системы автоматической фокусировки, то детектор сработает в случае, если сцена заслонена изображением сцены
Резкое изменение освещенности сцены (например, выключение света)	<u>Заслонение/затемнение:</u> До изменения режима наблюдения камеры (темнота при выключении света, засвет при включении) будет срабатывать детекция заслонения. <u>Расфокусировка:</u> При автоматической настройке камеры к новым условиям освещенности сцены может возникать кратковременная расфокусировка.
Ночной режим наблюдения	<u>Заслонение/затемнение:</u> В ночном режиме детекция заслонения работает так же, как и при дневном режиме, но могут возникать ситуации, когда объект на относительно большом расстоянии от камеры будет вызывать детекцию заслонения. <u>Расфокусировка:</u> Аналогично дневному режиму работы камеры.
Погодные условия, осложняющие видимость	<u>Заслонение/затемнение:</u> Капли на объективе, сильный дождь, песчаная буря и другие подобные этим явления, возникающие на сцене за короткий промежуток времени, могут вызвать детекцию заслонения. <u>Расфокусировка:</u> Вода на объективе может приводить к детекции.

Режим	Описание
Дневное освещение, неоднотонный фон, стабильная работа канала передачи видеопотока	Фиксируются начало и окончание смещения сцены. Используется коэффициент сглаживания, позволяющий игнорировать события с малыми изменениями состояния. Например, легкая вибрация камеры от проезжающей мимо машины не приведёт к срабатыванию события
Полное заслонение камеры и движение заслоняющего неоднотонного объекта перед камерой	Заслоняющий объект через некоторое время начнет восприниматься детектором как новая сцена, и движение объекта будет вызывать детекцию смещения
Частичное заслонение сцены	Если на незаслонённой части сцены есть чёткие края объектов, будет срабатывать детекция смещения.
Светящиеся объекты на сцене	Событие сдвига камеры может детектироваться в следующих случаях: - при движении человека в одежде со светоотражающими элементами; - при движении сильного источника света (засвета) или при сильном изменении освещенности объектов сцены.
Ночной режим наблюдения	При движении объектов на сцене возможно возникновение ложных срабатываний детекции
Погодные условия, осложняющие видимость	Продолжительные ливень, ураган, песчаная буря и т.п. могут привести к изменению сцены, и изменения на новой сцене могут вызывать срабатывание детекции

Настройка

Настройка производится в разделе **Управление → Устройства → Камеры** → клик на камере в списке → вкладка **Видеоаналитика**. Детектор расположен на главном экране мастера добавления детекторов.

Вмешательство в работу камеры



⚙️
▶
🕒

Поток ⓘ

640×480@fps24,H264

Чувствительность к заслонению и расфокусировке

Средняя

Чувствительность к сдвигу и тряске

Средняя

Назад

Готово

Параметр	Описание
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 960×540
Чувствительность	Уровень чувствительности детектора

Детектор оставленных предметов

Детектор обнаруживает на сцене предметы, оставленные без присмотра, и формирует тревогу, если объект находится в кадре без владельца дольше установленного времени. Тревога формируется только на предметы, которые были принесены человеком, что позволяет исключить из анализа предметы, которые изначально стояли на сцене (мусорные баки, лавочки и т.п.).

После того как объект остался в статичном положении и его владелец покинул зону рядом с объектом, запускается таймер. Если объект остаётся неподвижным в течение времени, заданного в настройках, он признаётся оставленным и детектор формирует тревогу.

Если объект был убран или к нему вернулся владелец до истечения таймера — счётчик сбрасывается и тревога не формируется.

В режиме поиска подозрительных предметов тревога также формируется при обнаружении предметов, которые изначально отсутствовали на сцене, а затем появились, и владелец которых не был идентифицирован. Этот режим удобно применять, например, для обнаружения подозрительных предметов, которые могли быть намеренно подброшены на сцену кем-то, стоящим вне поля зрения камеры.

Рекомендуется запускать детектор при максимально пустой сцене, насколько это возможно.

Условия работы

Детектор работает корректно при следующих условиях:

- сцена камеры хорошо освещается;
- объекты контрастны по отношению к фону;
- объекты находятся в фокусе камеры;
- объект занимает не менее 5% от площади кадра;
- камера расположена стационарно и хорошо закреплена.

При несоблюдении данных условий качество детекции может ухудшиться.

Детектируются объекты, удовлетворяющие условиям:

- расстояние до камеры — от 5 до 30 метров;
- объём объекта — более 3 дм³;
- размер на изображении — в пределах настроенного диапазона.

Объекты, не соответствующие этим критериям, игнорируются.

Настройка

Настройка производится в разделе **Управление → Устройства → Камеры →** клик на камере в списке → вкладка **Видеоаналитика**. Детектор расположен на главном экране мастера добавления детекторов.

Общие настройки

Параметр	Описание
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 960×540
Реагировать через, сек.	Время, в течение которого объект может оставаться без владельца в неподвижном состоянии, до момента формирования тревоги. Значение от 1 до 300 секунд
Определять подозрительные предметы	Расширенный режим детекции объектов, при котором тревога инициируется при обнаружении объекта, отсутствующего на сцене ранее
Время автоматического завершения события	Если событие длится дольше указанного времени, тревога будет сгенерирована повторно, чтобы в списке событий появилась более свежая запись с новым скриншотом

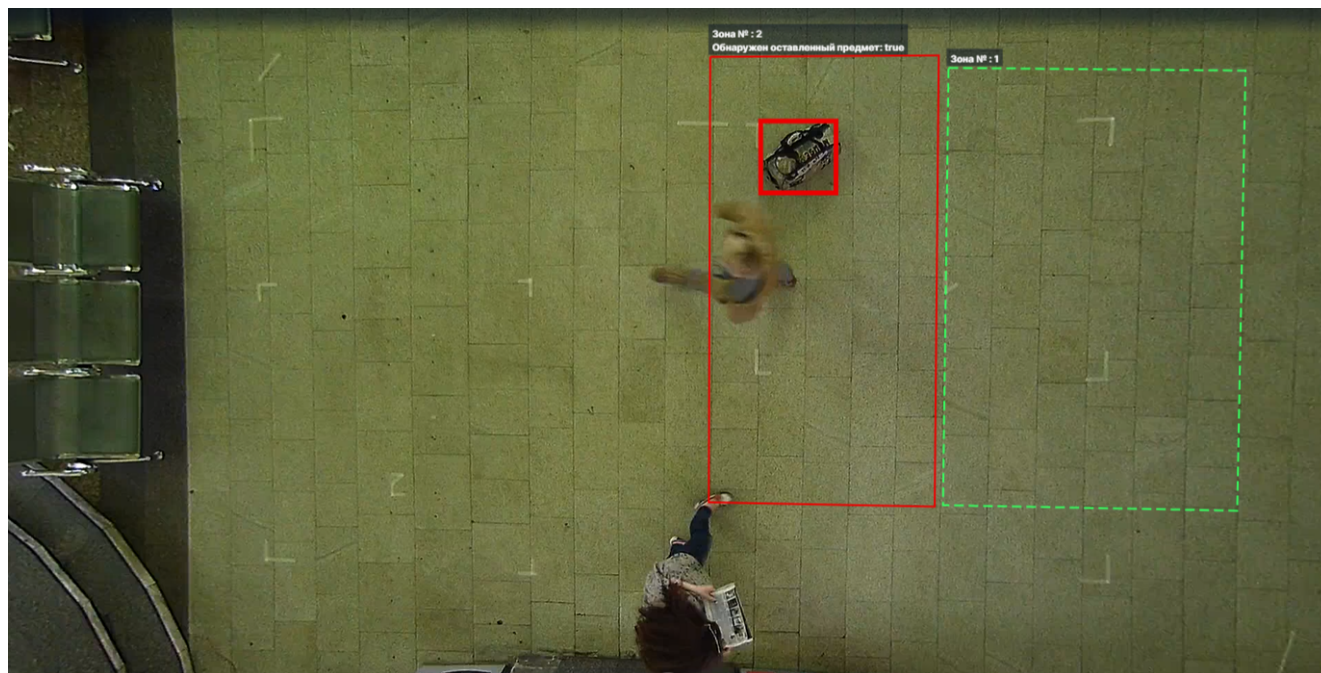
Разметка

Параметр	Описание	Настройка
Зона интереса	Область, в которой детектируются предметы	Разметка
Минимальный размер предмета	Предметы меньшего размера не будут детектироваться	Разметка
Максимальный размер предмета	Предметы большего размера не будут детектироваться	Разметка

Отображение тревоги при видеонаблюдении

При видеонаблюдении пунктиром отображается разметка границы зоны интереса и подпись с номером зоны. В случае тревоги и до момента окончания события граница зоны, в которой обнаружен оставленный предмет, отображается сплошной красной линией.

Если зона интереса не указана, то в случае тревоги красной линией обводится только обнаруженный предмет и показывается аннотация в левом верхнем углу видеоокна: «Обнаружен оставленный предмет».



Карточка события

В карточке события сохраняется скриншот с оповещением «Обнаружен оставленный предмет». Объект на сцене обводится рамкой. В карточке указывается тип тревоги и номер зоны, если зона интереса была настроена.

Оставленные предметы V3

Скриншот события
Плеер
Карта

Источник

Зона №

Обнаружен оставленный предмет

ABODA_554_109

1

Оповещение о движении в кадре

Детектор оповещает о движении в кадре.

Условия работы

Детектор работает корректно при следующих условиях:

- сцена камеры хорошо освещается;
- объекты контрастны по отношению к фону;
- объекты находятся в фокусе камеры;
- объект занимает не менее 5% от площади кадра;
- камера расположена стационарно и хорошо закреплена.

При несоблюдении данных условий качество детекции может ухудшиться.

Настройка

Настройка производится в разделе **Управление → Устройства → Камеры** → клик на камере в списке → вкладка **Видеоаналитика**. Детектор расположен на главном экране мастера добавления детекторов.

Общие настройки

Параметр	Описание
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 960×540
Длительность тревоги	Время, в течение которого тревога остается активной после прекращения движения на сцене. Значение от 1 до 60 секунд
Чувствительность к изменениям на сцене	Уровень чувствительности детектора к изменениям на сцене

Разметка

Параметр	Описание	Настройка
Зона интереса	Если задана зона, то только срабатывания детектора в этой области попадут в отчёты и сохранятся в базе. При этом детектор продолжит работать на всей площади кадра	Разметка
Минимальная площадь объекта	Объекты меньшего размера не будут детектироваться [	Разметка]

Отображение тревоги при видеонаблюдении

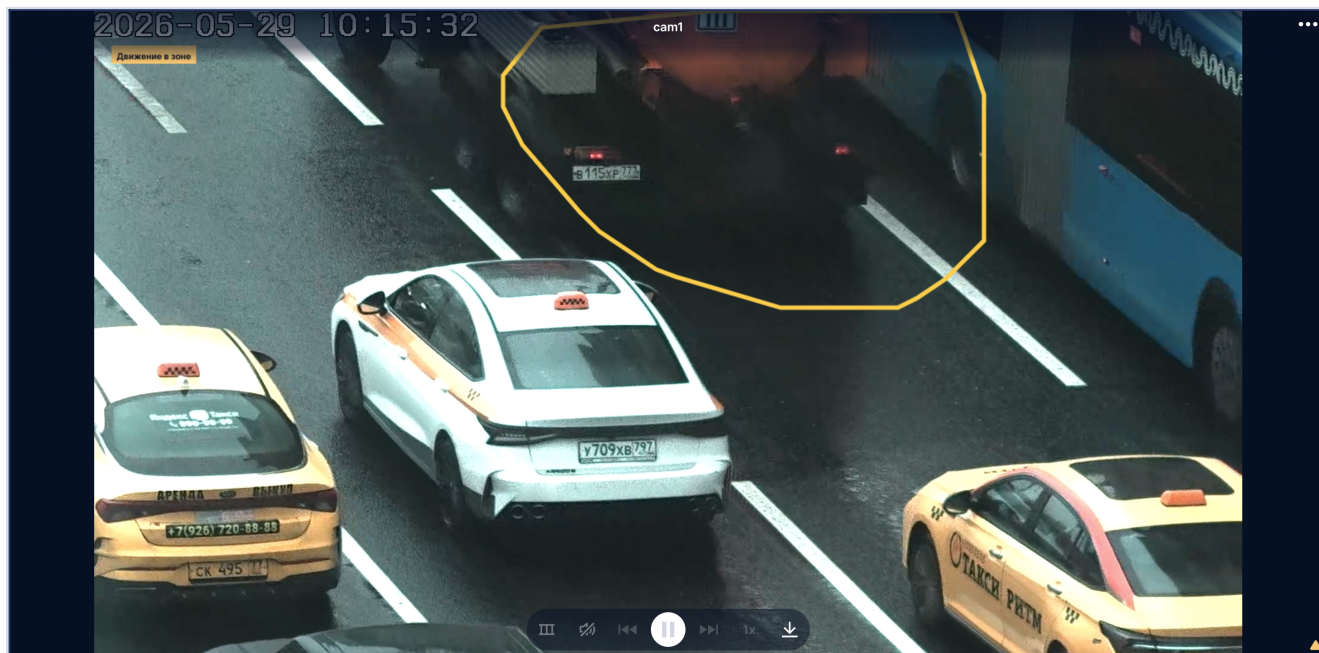
Тревога формируется только по срабатыванию детектора внутри отмеченной зоны интереса.

Отображение зоны интереса:

- сплошной красной линией — если в зоне обнаружена тревога;
- пунктирной зеленой линией — если в зоне нет тревоги.

При возникновении события в левом верхнем углу видеоокна появляется сообщение «Движение в зоне». Сообщение остаётся видимым в течение времени, заданном в параметре «Длительность тревоги».

Желтый многоугольник показывает объект детекции.

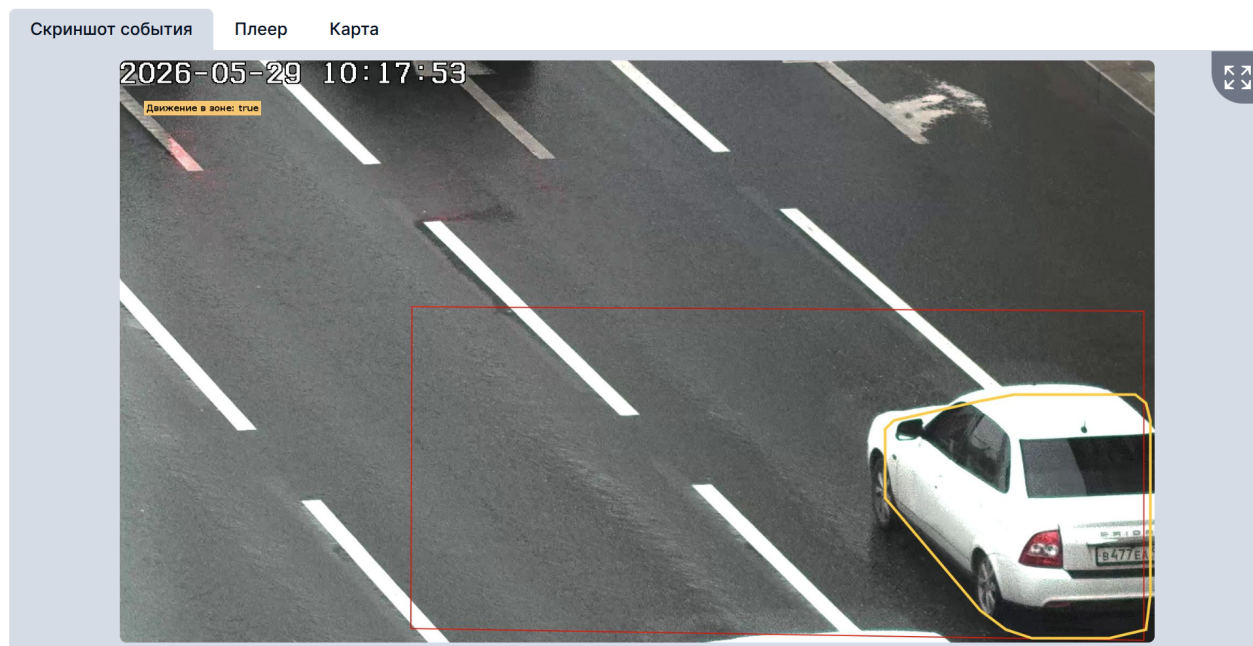


Карточка события

В карточке события сохраняется скриншот с оповещением «Движение в зоне». На скриншоте события объект движения обведен желтым многоугольником рамкой. В карточке указывается источник, тип тревоги и номер зоны, если зона интереса была настроена.

29.05.2026, 12:17:54 - 12:18:39

Оповещение о движении в кадре



Источник

cam1

Зона

1

Движение в зоне

Встроенная аналитика камеры

Встроенная аналитика камер поддерживается только в редакциях Professional и Enterprise. В остальных редакциях доступна только видеоаналитика Insentry.

ONVIF: вмешательство в работу камеры

Встроенная аналитика камер поддерживается только в редакциях Professional и Enterprise. В остальных редакциях доступна только видеоаналитика Insentry.

Детектор оповещает о попытке вмешательства в работу камеры.

Детектор отслеживает следующие типы событий:

- заслонение,
- затемнение,
- расфокусировка камеры,
- поворот,
- тряска.

Настройка производится в разделе **Управление → Устройства → Камеры** → клик на камере в списке → вкладка **Видеоаналитика**. Детектор расположен в папке **Встроенная аналитика камеры**.

Вмешательство в работу камеры



Поток

1920x1080@fps25,H264

Назад

Готово

Параметр	Описание	Тип	Настройка
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора	Обязательный	Выбор из списка

Этот детектор работает помощью встроенных средств камеры. Чтобы он работал корректно, камера должна поддерживать ONVIF протокол с профилем Т. Проверить поддержку этого профиля можно по Product name камеры: <https://www.onvif.org/conformant-products/>. Важно, что версия прошивки на камере должна быть не ниже той, с которой камера была сертифицирована для поддержки ONVIF.

Product Search

Application Type

Select

Profile(s)

Select

Manufacturer

Select

Product Name

DS-2CD2523G0-IS

Search



Поиск камеры

Export results to CSV



Showing 1 of 1 products

HIKVISION Hangzhou Hikvision Digital Technology

Product Name	Application Type	Profiles	Version	Date Approved
DS-2CD2523G0-IS	Device	G S T	V5.6.4 build 191224	2020-01-02

Прошивка на камере должна быть не ниже указанной в этом столбце - начиная с этой версии поддерживается профиль Т

Showing 1 of 1 products

Температура людей в кадре (интеграция с тепловизором Dahua)

Встроенная аналитика камер поддерживается только в редакциях Professional и Enterprise. В остальных редакциях доступна только видеоаналитика Insentry.

Детектор строит тепловую карту с отображением температуры людей. Чтобы детектор работал корректно, на камере должен быть тепловизор Dahua.

Настройка производится в разделе **Управление → Устройства → Камеры** → клик на камере в списке → вкладка **Видеоаналитика**. Детектор расположен в папке **Встроенная аналитика камеры**.



Параметр	Описание	Тип	Настройка
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора	Обязательный	Выбор из списка

ONVIF: движение в кадре

Встроенная аналитика камер поддерживается только в редакциях Professional и Enterprise. В остальных редакциях доступна только видеоаналитика Insentry.

Детектор оповещает, если обнаруживает движение в кадре.

Этот детектор работает помощью встроенных средств камеры. Чтобы он работал корректно, камера должна поддерживать ONVIF протокол с профилем Т. Проверить поддержку этого профиля можно по Product name камеры: <https://www.onvif.org/conformant-products/>. Важно, что версия прошивки на камере должна быть не ниже той, с которой камера была сертифицирована для поддержки ONVIF.

Product Search

Application Type
Select

Profile(s)
Select

Manufacturer
Select

Product Name
DS-2CD2523G0-IS
Поиск камеры

Search

Export results to CSV

Showing 1 of 1 products

HIKVISION Hangzhou Hikvision Digital Technology

Product Name	Application Type	Profiles	Version	Date Approved
DS-2CD2523G0-IS	Device	G S T	V5.6.4 build 191224	2020-01-02

Showing 1 of 1 products

Прошивка на камере должна быть не ниже указанной в этом столбце - начиная с этой версии поддерживается профиль T

Настройка производится в разделе **Управление → Устройства → Камеры** → клик на камере в списке → вкладка **Видеоаналитика**. Детектор расположен в папке **Встроенная аналитика камеры**.

Движение в кадре



07-11-2021 Sun 20:56:46

Камера 01

Поток
1920x1080@fps25,H264

Использовать нестандартные расширения камеры

Назад
Готово

Параметр	Описание	Тип	Настройка
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора	Обязательный	Выбор из списка

Аналитика лиц и поведения людей

Движение людей в запрещённом направлении

Детектор отслеживает движение людей в направлении, обозначенном как запрещённое.

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia**, на **ATI Radeon** детектор работать не будет.

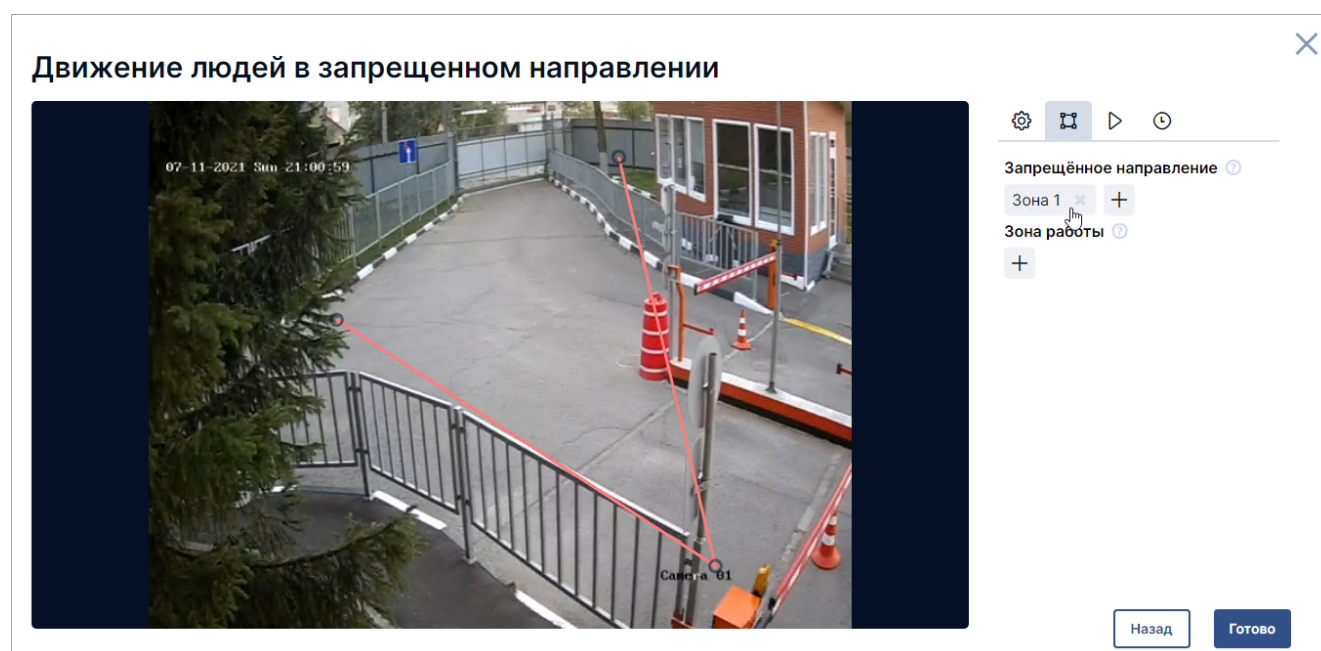
Условия работы

Детектор работает корректно при следующих условиях:

- сцена камеры хорошо освещается;
- объекты контрастны по отношению к фону;
- объекты находятся в фокусе камеры;
- объект занимает не менее 5% от площади кадра;
- камера расположена стационарно и хорошо закреплена.

При несоблюдении данных условий качество детектирования может ухудшиться.

Настройка производится в разделе **Управление → Устройства → Камеры →** клик на камере в списке → вкладка **Видеоаналитика**. Детектор расположен в папке **Люди → Обнаружение людей**.



Общие настройки

Параметр	Описание
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 640×360

Параметр	Описание
Режим запрещённого направления	Включено — детектор оповещает, когда человек идёт в направлении стрелки. Выключено — детектор оповещает, когда человек идёт в любом направлении, кроме указанного стрелкой
Время реакции, сек	Время, через которое сработает тревога после обнаружения нарушения направления движения. При значении 0 тревога срабатывает немедленно. Значение от 0 до 300 секунд
Допустимое отклонение, градусы	Допустимое отклонение от заданного направления движения в градусах. Меньшее значение означает более строгую проверку направления. Значение от 5° до 45°
Задержка отключения тревоги, сек	Время, в течение которого тревога остается активной после прекращения нарушений направления движения. Значение от 1 до 300 секунд
Показывать треки движения	Включено — на видео отображаются треки движения. Выключено — показаны только маркерные точки людей
Проверять сцену	Частота проверки сцены

Разметка кадра

Параметр	Описание	Тип	Настройка
Зона интереса	Если область задана, то только срабатывания детектора в этой области попадут в отчёты и сохранятся в базе. При этом детектор продолжит работать на всей площади кадра. Можно задать несколько зон. В карточке события отображается, в какой зоне зафиксировано событие	Необязательно	Вкл. метка
Контрольные линии	Стрелка обозначает направление движения. Если задана зона интереса, то линия должна находиться полностью внутри зоны. Количество зон должно совпадать с количеством линий. Зоны и линии работают попарно: зона 1 — линия 1, зона 2 — линия 2 и так далее	Необязательно	Вкл. метка

Детектор людей в запрещённой зоне

Детектор отслеживает нахождение людей в области, отмеченной как запрещённая. При обнаружении движения в запрещённой зоне, детектор отправляет оповещение и отмечает область, где происходит движение.

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia**, на **ATI Radeon** детектор работать не будет.

Детектор работает корректно при следующих условиях:

1. сцена камеры хорошо освещается;
2. объекты контрастны по отношению к фону;
3. объекты находятся в фокусе камеры;
4. объект занимает не менее 5% от площади кадра;

5. камера расположена стационарно и хорошо закреплена.

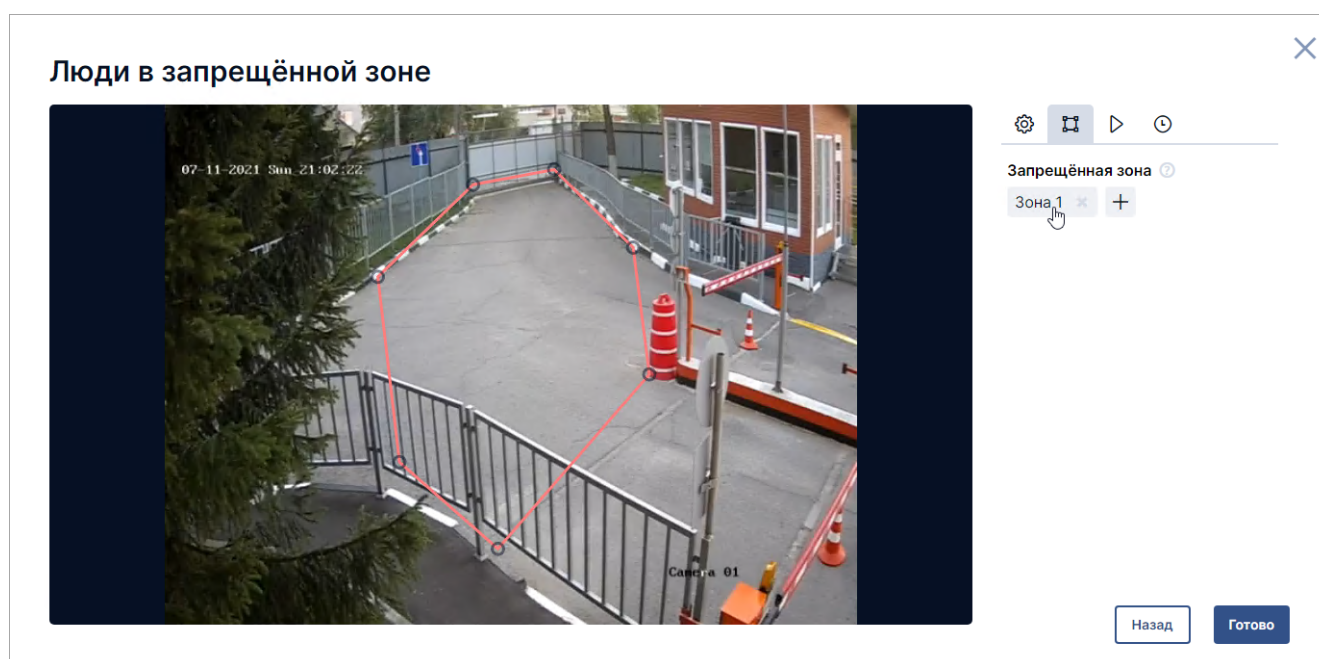
При несоблюдении данных условий качество детектирования может ухудшиться.

Особенности работы детектора:

1. Если человек зайдет в запретную зону и там закроет от обзора камеры контрольную точку (например, закроет ноги пакетом при съемке сбоку или откроет зонт при съёмке сверху), то при пропадании контрольной точки из поля зрения камеры детекция нахождения человека прекратится — для детектора зона станет чистой.
2. Если человек проедет по стерильной зоне, например, на велосипеде так, что ноги окажутся выше границы зоны, то детекции нахождения человека в запретной зоне не будет.
3. Не фиксируется пересечение зоны животными и машинами.
4. Если попытаться определить толпу, детекции не будет, т.к. люди, находящиеся перед границей зоны, заслоняют собой людей в запретной зоне.

Порядок настройки

Настройка производится в разделе **Управление → Устройства → Камеры →** клик на камере в списке **→** вкладка **Видеоаналитика**. Детектор находится в папке **Люди → Обнаружение людей**.



Общие настройки

Параметр	Описание	Тип	Настройка
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендованное разрешение: 640×360	Обязательный	Выбор из списка
Определять людей по	Точки, по которым определяются фигуры людей: шея, лодыжки, кисти рук, голова. Выбирайте те, которые лучше всего видны камере	Обязательный	Выбор из списка
Проверять сцену	Частота проверки сцены. Чем ниже, тем меньше нагрузка на ресурсы компьютера	Обязательный	Выбор из списка

Разметка кадра

Параметр	Описание	Тип	Настройка
Запрещённая зона	Область, которую детектор будет считать запрещённой. Можно задать несколько зон. В карточке события и в оповещении отображается, в какой зоне детектор обнаружил человека	Обязательный	Разметка Зона должна быть замкнутой, поэтому последняя точка должна совпадать с первой

Детектор очередей

Детектор предназначен для мониторинга и анализа потоков клиентов в зонах обслуживания (кассы, банкоматы, стойки обслуживания и др.).

Детектор: 1. Подсчитывает и отображает текущее количество людей в очереди. 1. Оповещает, если очередь длиннее заданного числа человек. 2. Рассчитывает метрики эффективности обслуживания: * количество обслуженных клиентов; * среднюю интенсивность обслуживания (количество человек в минуту).

События и метрики позволяют отреагировать на перегрузку и проводить ретроспективный анализ загруженности.

Особенности детектора:

1. Для каждого трека человека производится учёт времени пребывания в зоне обслуживания. Время учитывается от первого входа до последнего выхода, даже если между ними была потеря детекции. Для разных зон обслуживания ведётся отдельный хронометраж.
2. Объект учитывается в метриках только после нахождения в зоне очереди не менее 10 секунд.

3. Пороговое значение максимальной длины очереди задаётся общее для всех зон. Событие при превышении заданного порога числа людей в очереди завершается после того как на протяжении 10 секунд число людей в очереди ниже порогового значения.
4. В карточке события отображаются агрегированные метрики для зоны очереди на основе данных входящих в неё зон обслуживания.

Детектор работает корректно при следующих условиях:

- Камера размещена сбоку, допускается размещение ~30% от перпендикуляра к условной линии очереди.
- Камера закреплена статично под углом 45-60° на высоте 3-4 метра над чётко обозначенной зоной ожидания (согласно разметке) с постоянным искусственным освещением.
- В кадре нет движущихся фоновых объектов (эскалатора, мерцающего экрана с изображениями и т.д.).
- Люди выстраиваются в предсказуемую линию (тип очереди «линейный»).
- Зона обслуживания не загорожена сторонними объектами (рекламными/информационными стойками, мониторами, колоннами и т.п.).
- Зоны обслуживания не накладываются друг на друга.
- Люди в зоне обслуживания наблюдаются в полный рост.

При несоблюдении данных условий качество детекции может ухудшиться.

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia**, на **ATI Radeon** детектор работать не будет.

Настройка производится в разделе **Управление → Устройства → Камеры →** клик на камере в списке **→** вкладка **Видеоаналитика**. Детектор расположен в папке **Люди → Обнаружение людей**.

Общие настройки

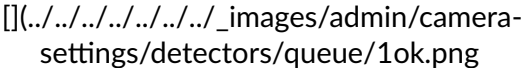
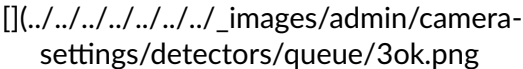
Параметр	Описание	Тип	Настройка
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 640×360	Обязательный	Выбор из списка
Оповещать, если людей в очереди более	Если в очереди будет больше (≥) человек, чем указано в этой настройке, детектор создаст оповещение	Обязательный	Целое число от 2 до 100

Разметка кадра

Параметр	Описание	Настройка
Зона очереди	Зона очереди охватывает пространство, где люди выстраиваются в очередь к точке обслуживания. Внутри этой зоны детектор определяет длину очередей и генерирует событие, если людей в очереди слишком много. В одну зону могут входить несколько очередей, тогда у них будет общая статистика по количеству людей, но отдельные метрики обслуживания. Если зона не задана, зоной очереди считается вся площадь кадра. Если зона задана, она должна обязательно содержать хотя бы одну зону обслуживания	Разметка
Зона обслуживания	В этой зоне рассчитываются метрики обслуживания людей. Зона должна входить в зону очереди и охватывать область обслуживания клиента. Чтобы метрики отдельной зоны считались без ошибок, расположите зону так, чтобы в неё не входили люди из других зон и проходящие мимо. Зона обслуживания должна располагаться минимум на 90% внутри зоны очереди, если она задана	Разметка

Рекомендации по настройке зон

Корректные настройки зон

Пример	Пояснение
	) Для каждой зоны обслуживания задана своя зона очереди
	) У зон обслуживания 1 и 2 общая зона очереди. У них общая статистика по количеству обслуженных людей, но отдельные метрики эффективности обслуживания
	) Ни у одной зоны обслуживания нет зоны очереди. В этом случае зоной очереди считается весь кадр и для всех зон обслуживания статистика по количеству людей в очереди будет общей
	) У каждой зоны обслуживания есть зона очереди. Зоны очередей могут пересекаться, но лучше этого избегать

Некорректные настройки зон

Пример	Пояснение
 (../..../..../..../_images/admin/camera-settings/detectors/queue/2nok.png	) Если зоны очереди заданы, то они должны быть обозначены для каждой зоны обслуживания
 (../..../..../..../_images/admin/camera-settings/detectors/queue/1nok.png	) Зона очереди должна содержать внутри себя хотя бы одну зону обслуживания. Зона обслуживания минимум на 90% должна располагаться внутри зоны очереди, если она задана

Детектор толпы

Детектор фиксирует возникновение столпотворения людей, оповещает об этом и отмечает расположение толпы на кадре. В карточке события выводится число обнаруженных людей и предельное число людей в зоне интереса, по которой получено событие.

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia**, на **ATI Radeon** детектор работать не будет.

Выберите детектор в списке в левой части экрана. Справа будут представлены его настройки. Настройка производится в разделе **Управление → Устройства → Камеры →** клик на камере в списке → вкладка **Видеоаналитика**.

Настройка

Общие настройки

Параметр	Описание	Тип	Настройка
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 640×360	Обязательный	Выбор из списка
Минимальный размер толпы	Минимальное число людей, которое будет детектироваться, как толпа	Обязательный	Целое положительное число
Показывать маркеры людей в толпе	Отмечать маркерами каждого человека в обнаруженном скоплении людей	Необязательный	Включить/выключить
Чувствительность	Уровень чувствительности детектора к изменениям на сцене	Обязательный	Выбор из списка

Параметр	Описание	Тип	Настройка
Время автоматического завершения события	Если событие длится дольше указанного времени, тревога будет сгенерирована повторно, чтобы в списке событий появилась более свежая запись с новым скриншотом	Обязательный	Выбор из списка

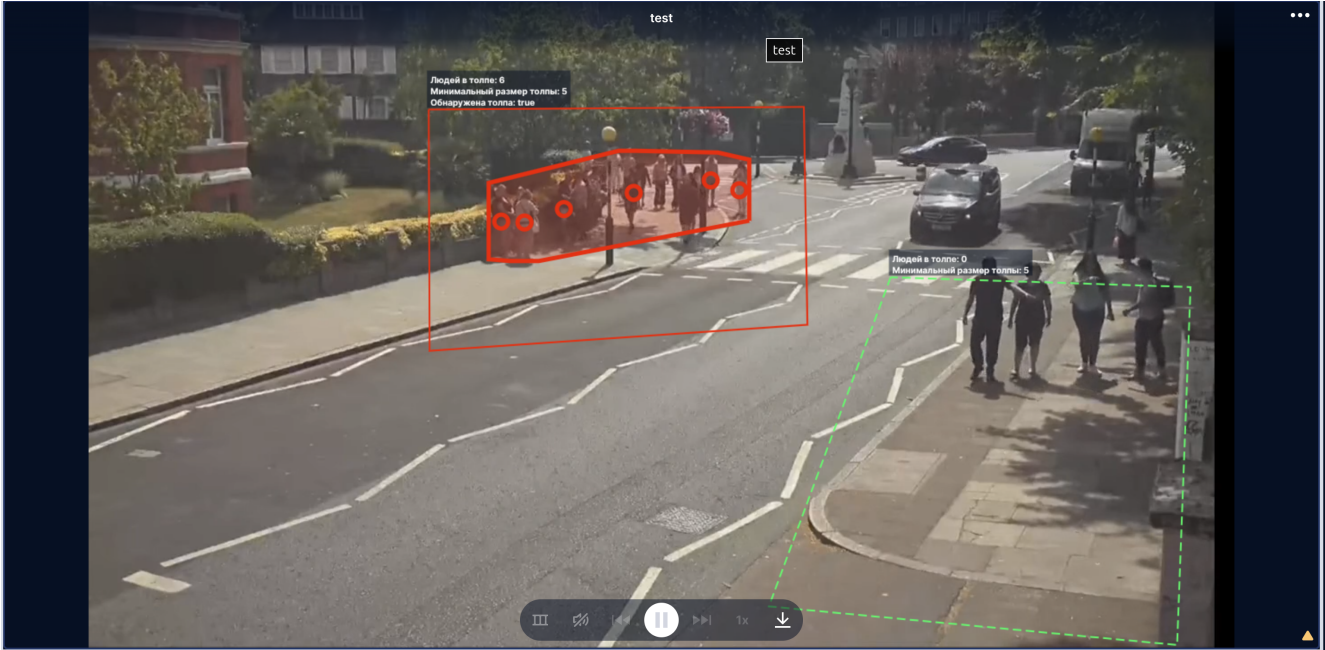
Разметка

Параметр	Описание	Тип	Настройка
Зона интереса	Если область задана, то только срабатывания детектора в этой области попадут в отчёты и сохранятся в базе. При этом детектор продолжит работать на всей площади кадра	Необязательный	Виджет Зона должна быть замкнутой, поэтому последняя точка должна совпадать с первой

Отображение тревоги при видеонаблюдении

При видеонаблюдении пунктиром отображается разметка границы зоны интереса. В случае тревоги и до момента окончания события граница зоны, в которой обнаружена толпа, отображается сплошной красной линией.

Если зона интереса не указана, то в случае тревоги красной линией и заливкой обводится только область, в которой обнаружено скопление людей, превышающее допустимый порог. В аннотации в левом верхнем углу видеоокна показан текст тревоги: «Обнаружен оставленный предмет», а также минимальный размер толпы и зафиксированное количество людей в толпе.



Карточка события

В карточке события сохраняется скриншот с оповещением «Обнаружена толпа». Толпа на сцене обводится красной рамкой и заливкой. Если зона интереса была настроена, и в ней обнаружена

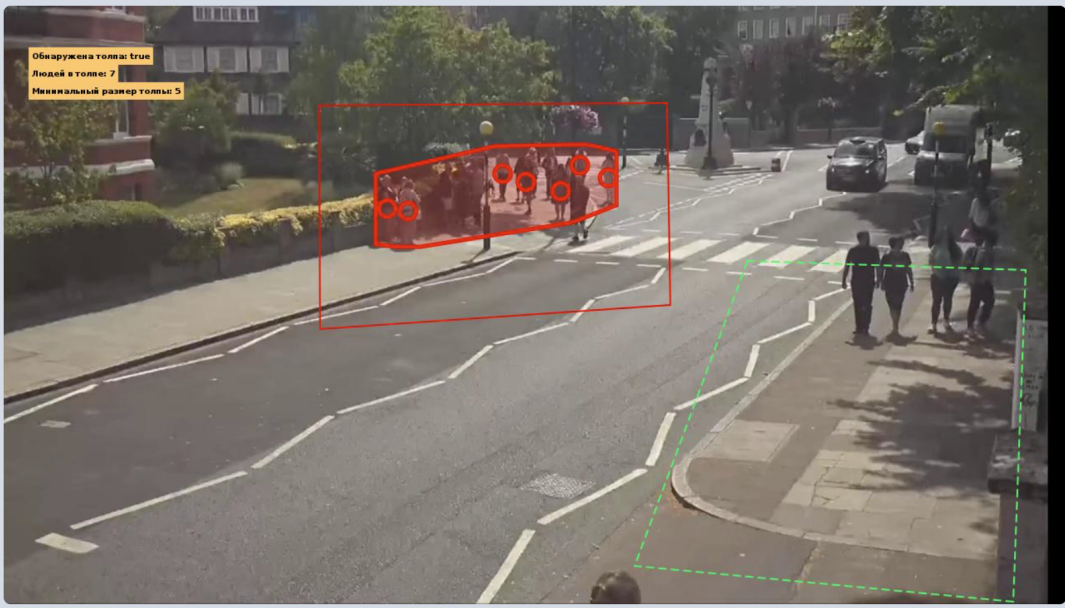
толпа, то границы зоны выделены красным цветом. Если включена настройка «Показывать маркеры людей в толпе», то фигуры людей внутри толпы отмечены маркерами.

В аннотации и в описании события указан минимальный размер толпы и зафиксированное количество людей в толпе.

29.05.2026, 11:47:10 - 11:47:10

Толпа

Скриншот события Плеер Карта



Источник test

Людей в толпе	7
Минимальный размер толпы	5
Обнаружена толпа	

Подсчёт людей

Детектор считает количество вошедших и/или вышедших людей, пересекающих заданную линию. Результат работы детектора отображается в отчёте (см. *Руководство пользователя*, раздел *Отчёты*).

Как правило, этот детектор используется для подсчёта посетителей: контрольная линия располагается на входе в помещение, и детектор считает количество вошедших и вышедших людей.

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia**, на **ATI Radeon** детектор работать не будет.

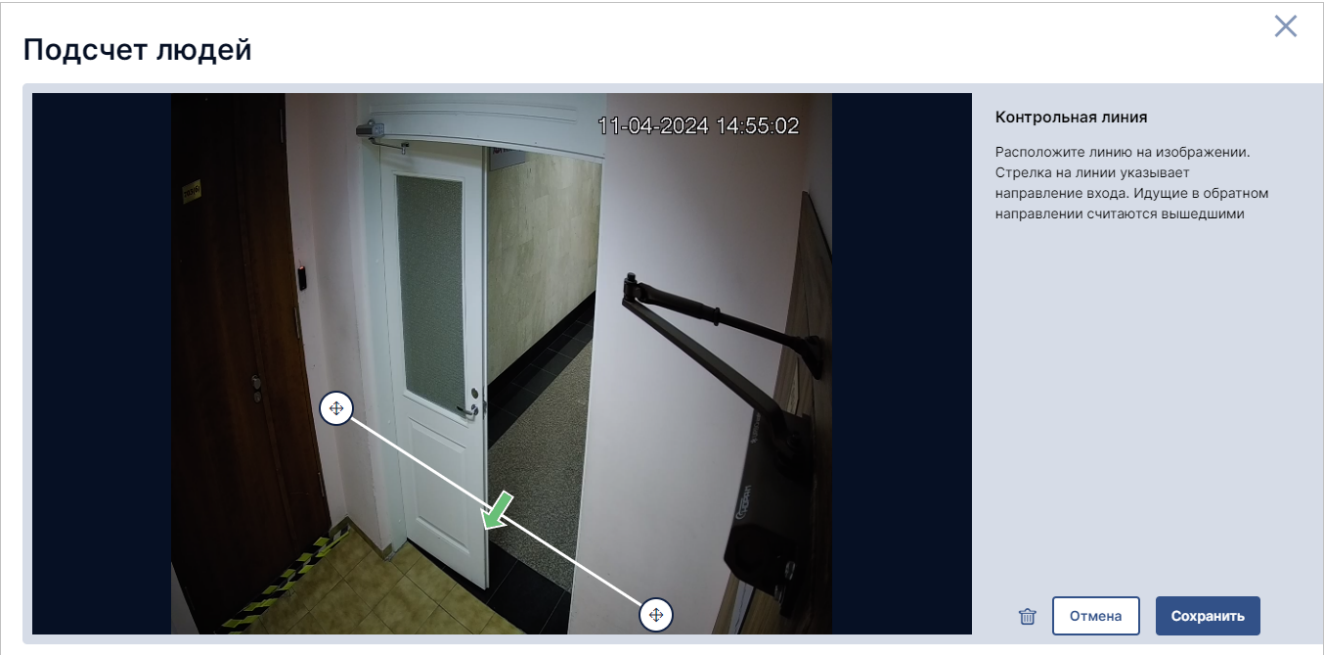
Условия работы детектора

Детектор работает корректно при следующих условиях:

- дневное освещение;
- контрастное изображение;
- корректная фокусировка камеры;
- объекты аналитики хорошо различимы и идентифицируются как люди;
- камера находится под углом от 30 до 60 градусов в 3—6 метрах над областью аналитики;

- область аналитики горизонтальная.

Настройка производится в разделе **Управление → Устройства → Камеры → Настройки камеры → Видеоаналитика**. Детектор расположен в папке **Люди → Обнаружение людей**.



Общие настройки

Параметр	Описание
Поток	Если у камеры несколько потоков, возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками. Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 640×360
Считать количество	Выбор метода подсчёта для сбора статистики: только вошедшие люди, только вышедшие или все
Выводить подробную информацию о работе детектора	Выводить диагностический интерфейс и отмечать треки людей разноцветными линиями в окне просмотра камеры

Разметка кадра

Параметр	Описание	Настройка
Контрольная линия	Детектор будет считать количество людей, пересекающих линию. Стрелка обозначает направление входа. Люди, пересекающие линию в обратном направлении, будут считаться вышедшими	Разметка

Параметр	Описание	Настройка
Зона детекции	Если область не задана, то областью детекции считается вся площадь кадра. Ограничение зоны повышает стабильность работы детектора	Разметка

Диагностический интерфейс

Если включена настройка **Выводить подробную информацию о работе детектора**, в окне просмотра камеры с запущенным детектором будет показан диагностический интерфейс с подобной информацией о показателях работы детектора.



Трек человека — то, как детектор «видит» путь человека в кадре. Треки людей отмечаются цветными линиями:

- зелёный — люди, которые ещё не пересекли контрольную линию (детектор увидел человека, но ещё не засчитал пересечение линии);
- синий — вошедшие люди;
- красный — вышедшие люди.

Матчинг — процесс, при котором детектор «узнаёт», что на двух последовательных кадрах один и тот же человек. Если детектор плохо справляется с этим, он будет работать неверно: например, посчитает пересечение линии одним человеком как несколько пересечений, приняв его за разных людей. Значение матчинга показывает условное расстояние в пикселях, которое проходит человек в зоне интереса, пока детектор при смене кадров продолжает идентифицировать его как одного и того же человека.

Показатели на диагностическом интерфейсе:

- **Вошло** — количество вошедших людей (пересечение контрольной линии в прямом направлении);
- **Вышло** — количество вышедших людей (пересечение контрольной линии в обратном направлении);
- **Среднее значение матчинга** — среднее значение матчинга среди последних 10 тыс. срабатываний;

- **Максимальное значение матчинга** — максимальное значение матчинга среди последних 2500 срабатываний;
- **90-й процентиль** — 90% зафиксированных детектором пересечений контрольной линии были определены со значением матчинга менее или равным значению, указанному в этом показателе;
- **Разница между средним и 90-м процентилем** — значение в процентах, на которое 90-й процентиль больше среднего значения матчинга.

Подсчёт вошедших и вышедших людей начинается сразу после запуска детектора. Остальные диагностические показатели начнут отображаться после того как детектор обработает первые 500 кадров с перемещающимися людьми (даже если это будет один и тот же человек).

Для диагностики работы детектора:

1. После запуска детектора посмотрите на треки людей в кадре и счётчики вошедших/вышедших людей. Убедитесь, что детектор верно распознаёт движение людей: при пересечении контрольной линии одним человеком, счётчик должен увеличиваться на единицу.
2. Подождите 3—5 минут после запуска детектора (перед камерой в это время должен ходить хотя бы один человек) и проверьте счётчики вошедших и вышедших людей ещё раз. Если всё верно, зафиксируйте текущие диагностические показатели как плановые.
3. Если позже вы заметите, что показатели сильно отличаются от плановых — значит, что-то идёт не так. Например, значение разницы между 90-м и средним перцентилем может сильно увеличиться, если люди перед камерой начнут массово бежать или прятаться за объектами. Если люди идут с обычной скоростью, а показатели сильно отклоняются от плановых, значит, детектор некорректно настроен или плохо работает. В этом случае проверьте: * расположение контрольной линии в настройках детектора; * калибровку камеры; * расположение и угол наклона камеры — чтобы детектор правильно определял людей в кадре, зона интереса должна быть хорошо освещена, камера должна корректно фокусироваться.

Детектор касок

Детектор оповещает оператора, если в зоне интереса камеры находится человек, на голове которого с высокой вероятностью отсутствует каска.

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia**, на **ATI Radeon** детектор работать не будет.

Условия работы детектора:

- лицо человека занимает не более 20% площади экрана;
- люди находятся не далее чем в 50 метрах от камеры;
- голова человека полностью попадает в зону интереса и ничем не загорожена;
- угол наклона камеры от 30 до 60 градусов относительно линии горизонта.

Настройка производится в разделе **Управление → Устройства → Камеры → Настройки камеры → Видеоаналитика**. Детектор расположен в папке **Люди → Средства индивидуальной защиты**.

Общие настройки

Параметр	Описание
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 960×540

Разметка кадра

Параметр	Описание	Тип	Настройка
Зона работы	Область задаётся на изображении камеры. Если область не задана, то областью детекции считается вся площадь изображения	Необязательный	Войметка Зона должна быть замкнутой, поэтому последняя точка должна совпадать с первой

Распознавание лиц

Детектор распознаёт лица проходящих мимо камеры людей и сохраняет их в общую базу. Если добавить в [список персон](#) человека, чьё лицо сохранено в базе детектора, будут сформированы карточки ранее зафиксированных событий с этим человеком — с фотографиями, датой и временем. Лица из базы не удаляются.

База лиц хранится локально и может занять много места на диске.

При распознавании лица детектор может генерировать оповещения, которые появятся на таймлайне в разделе **Просмотр**. Информация о событии сохраняется в карточке события.

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia**, на **ATI Radeon** детектор работать не будет.

Настройка производится в разделе **Управление → Устройства → Камеры →** клик на камере в списке **→** вкладка **Видеоаналитика**. Детектор расположен в папке **Люди**.

Распознавание лиц

11-04-2024 15:02:34



Поток

704x576@fps25, H264

Сравнивать с фото

Нестрого

Генерировать оповещения

Ни о ком

Сохранять лица не из базы

☐

Показывать нераспознанные лица

☐

Назад

Готово

Общие настройки

Параметр	Описание
Поток	Если у камеры несколько потоков, возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками. Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 960x540
Сравнивать с фото	Выбирайте строгость сравнения в зависимости от того, кто ходит мимо камеры, и задач детектора. При распознавании лица детектор сравнит его с фотографиями людей в списке персон. При нестрогом сравнении ниже вероятность пропустить важного человека, зато больше ложных срабатываний
Генерировать оповещения	Варианты: О людях из списка / О людях не из списка / Обо всех / Ни о ком. В режиме «Обнаружение» оповещения работают так: если оповещения генерируются О людях из списка или Ни о ком, то оповещения не будут генерироваться. Если выбрать вариант О людях не из списка или Обо всех, то оповещения будут генерироваться при распознавании каждого человека

Параметр	Описание
Сохранять все лица	Если настройка включена, детектор будет пополнять базу, сохраняя лица всех проходящих мимо камеры людей. Будьте внимательны — база лиц хранится локально и может занять много места на диске, если мимо камеры ходит много людей не из списка персон. Лица из базы не удаляются. Если добавить в список персон человека, чьё лицо сохранено в базе детектора, будут показаны кадры ранее зафиксированных событий с этим человеком. Если настройка выключена, новые лица не будут сохраняться в базу
Показывать нераспознанные лица	На скриншотах оповещений будут отображаться серым цветом ещё не распознанные лица

Разметка кадра

Параметр	Описание	Настройка
Зона работы	Детектор будет срабатывать на предметы, полностью попадающие в отмеченные зоны. Предметы на границе зоны не будут детектироваться	Разметка Зона должна быть замкнутой, поэтому последняя точка должна быть установлена там же, где первая
Минимальный размер лица	Размер задаётся интерактивным овалом. Лица меньшего размера не будут детектироваться	Разметка

Детектор падения человека

Детектор фиксирует нахождение человека в горизонтальном или близком к горизонтальному положении, оповещает оператора и показывает местонахождение этого человека.

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia**, на **ATI Radeon** детектор работать не будет.

Условия работы детектора

- в зоне видимости камеры находятся две контрольные точки человека: основание шеи и центр таза. Если одна из точек загорожена или не попадает в зону видимости камеры, то положение человека не определяется;
- люди находятся не далее чем в 50 метрах от камеры;
- угол наклона камеры от 30 до 60 градусов относительно линии горизонта.

Настройка производится в разделе **Управление → Устройства → Камеры → Настройки камеры → Видеоаналитика**. Детектор расположен в папке **Люди → Поведение людей**.

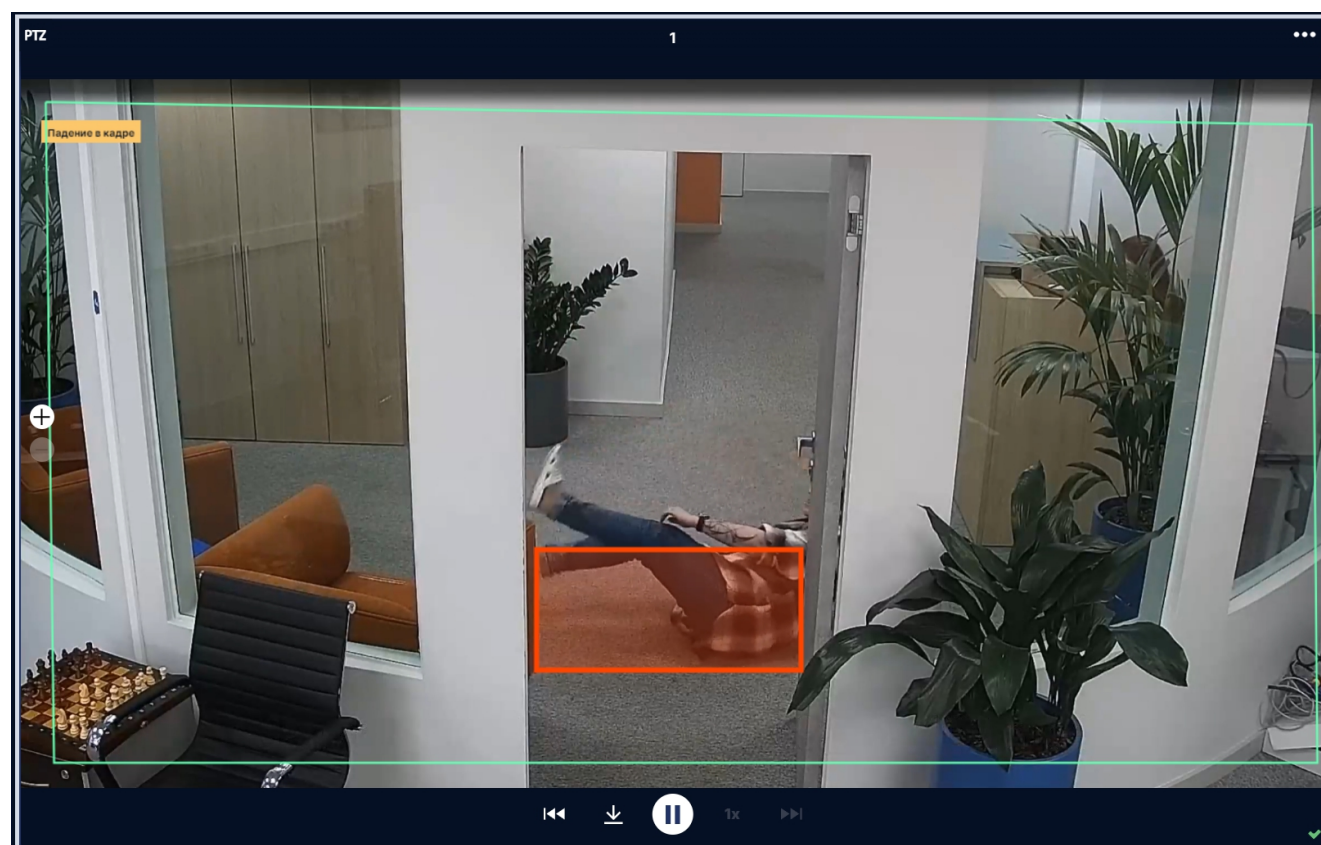
Общие настройки

Параметр	Описание
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 960×540

Разметка кадра

Параметр	Описание	Тип	Настройка
Зона работы	Область задаётся на изображении камеры. Если область не задана, то областью детекции считается вся площадь изображения	Необязательный	Виджет Зона должна быть замкнутой, поэтому последняя точка должна совпадать с первой

Пример работы

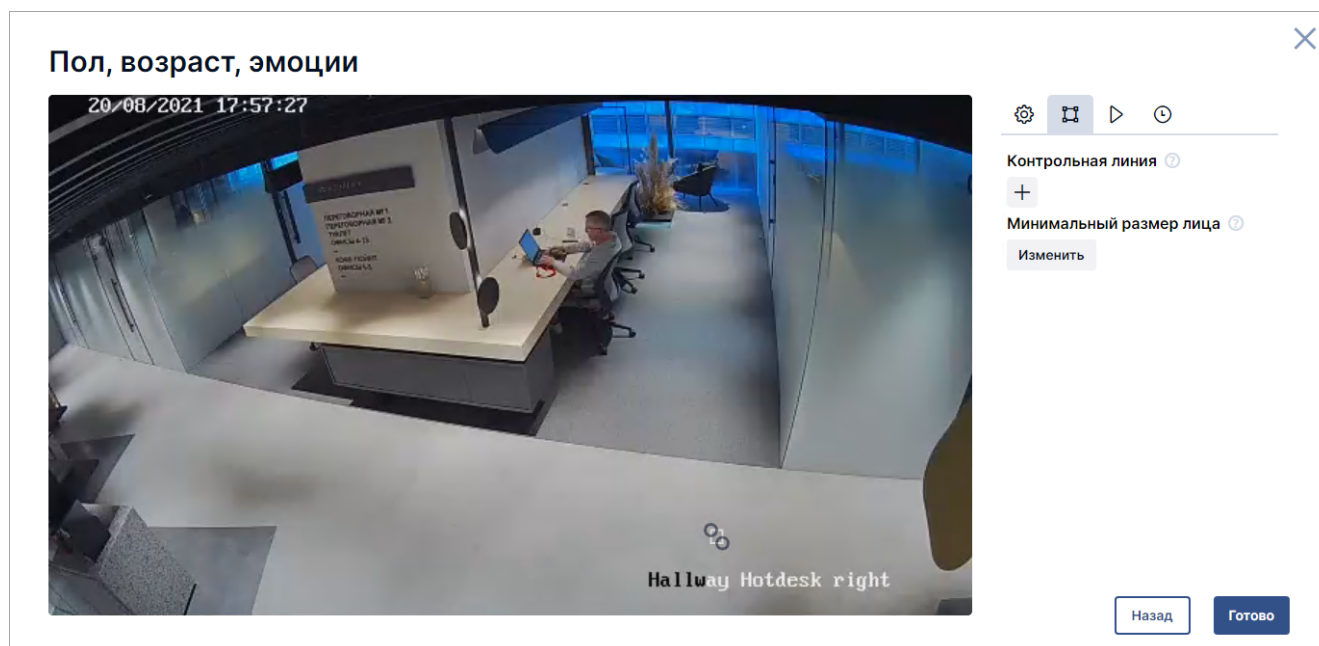


Пол, возраст, эмоции

Детектор определяет пол, примерный возраст и наиболее выраженную эмоцию каждого человека в кадре. На основе собранных данных строится отчёт (см. *Руководство пользователя*, раздел *Отчёты*).

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia**, на **ATI Radeon** детектор работать не будет.

Настройка производится в разделе **Управление → Устройства → Камеры → Настройки камеры → Видеоаналитика**. Детектор расположен в папке **Люди**.



Общие настройки

Параметр	Описание	Настройка
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуемое разрешение: 960×540	Выбор из списка

Разметка кадра

Параметр	Описание	Настройка
Контрольная линия	При пересечении этой линии человеком, информация о его поле, возрасте и эмоции сохраняется в статистику. Если линия не задана, то в статистику попадает информация обо всех людях в зоне работы детектора, чьи эмоции, пол и возраст были распознаны детектором	Разметка
Зона работы	Область задаётся на изображении камеры. Если область не задана, то областью детекции считается вся площадь изображения	Разметка Зона должна быть замкнутой, поэтому последняя точка должна совпадать с первой
Минимальный размер лица	Размер задаётся интерактивным овалом. Лица меньшего размера не будут детектироваться	Разметка

Детектор пересечения линии

Детектор формирует тревогу при обнаружении человека, пересекающего заданную линию.

Настройка

Настройка производится в разделе **Управление → Устройства → Камеры → Настройки камеры → Видеоаналитика**. Детектор расположен в папке **Люди**.

Общие настройки

Параметр	Описание	Настройка
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендованное разрешение: 960×540	Выбор из списка

Разметка

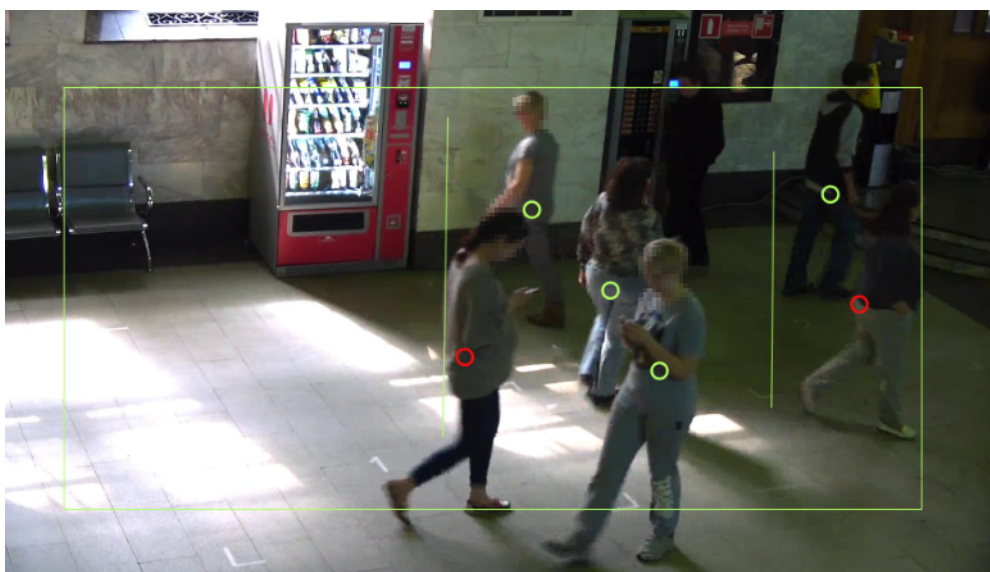
Параметр	Описание	Настройка
Зона детекции	Область задаётся на изображении камеры. Если область не задана, то областью детекции считается вся площадь изображения	Разметка Зона должна быть замкнутой, поэтому последняя точка должна совпадать с первой

Параметр	Описание	Настройка
Контрольная линия	При пересечении этой линии человеком, детектор генерирует тревогу	Разметка

Отображение тревоги при видеонаблюдении

При видеонаблюдении отображается разметка границы зоны детекции. Фигуры людей на сцене отмечены маркерами:

- зелёный — люди, не пересекшие линию;
- красный — люди, пересекшие линию.



Карточка события

В карточке события сохраняется скриншот с отметками людей, пересекших линию. Разметка отображается на скриншоте.

27.05.2026, 12:03:20

Пересечение линии

Скриншот события

Плеер

Карта



Источник

fob_dir_921_114

Аналитика транспорта**Детектор гос. номеров машин**

Детектор распознаёт и отображает номерные знаки автомобилей в кадре. Для российских номеров показан также тип распознанного номера. В карточке события показывается кадр целиком, а также обрезанная часть кадра, на которой хорошо виден распознанный номер.

Если автомобиль указан в [списке транспорта](#), события с автомобилем регистрируются и формируются карточки событий. По распознанным номерам можно сформировать отчёт.

Внимание! Для корректной работы детектора необходима видеокарта **Nvidia** не ниже **1050ti**, на **ATI Radeon** детектор работать не будет.

Условия детекции появления автомобиля:

- середина автомобиля попадает в область интереса камеры;
- угол между траекторией движения автомобиля и углом обзора камеры не превышает 30 градусов;
- камера расположена так, чтобы минимизировать засвет фарами;
- достаточное освещение.

Условия определения номерного знака:

- номерной знак определяется только при условии достаточной видимости. Если на кадре изображения знак различим глазами, то и камера его распознает;
- номерной знак расположен горизонтально (не более 15 градусов отклонения от линии горизонта).
- распознаются номерные знаки российского формата (ГОСТ Р 50577-2018).

Настройка производится в разделе **Управление → Устройства → Камеры** → клик на камере в списке → вкладка **Видеоаналитика**. Детектор расположен в папке **Автомобили**.

Распознавание гос. номеров машин

06-27-2024 Thu 14:13:32



Поток

1280x960@fps20, H264

Оповещение номера машины

☐

Показывать машины с нераспознанными номерами

☐

Распознавать номер повторно при улучшении его читаемости

Часто

Назад

Готово

Общие настройки

Параметр	Описание
Поток	Если у камеры несколько потоков , возможно выбрать, какой из них будет использован для данного детектора. Автоматически выбирается поток с наиболее подходящими характеристиками . Звёзды показывают, насколько поток подходит для видеоаналитики с точки зрения нагрузки на сервер. Чем ближе разрешение, частота кадров и кодек потока к требованиям детектора, тем выше оценка и тем меньше ресурсов будет тратиться впустую. Рекомендуется выбрать поток с разрешением 1920x1080
Оповещение номера машины	Если включено, в списке событий и на таймлайне будут созданы оповещения о каждом распознанном номере автомобиля
Показывать машины с нераспознанными номерами	На кадрах в оповещениях будут отображаться серым цветом машины, у которых еще не удалось распознать гос. номер
Распознавать номер повторно при улучшении его читаемости	Детектор непрерывно находит на сцене и распознаёт номерные знаки транспортных средств. Если ТС с уже распознанным уже распознанным номером приближается к камере или становится лучше освещён, то уверенность детектора в выдаваемом результате повышается. Низкий порог подходит, если нужна особая точность распознавания — детектор будет создавать новые события с обновлёнными номерами даже при небольшом изменении уверенности. Чем ниже порог, тем больше будет событий

Разметка

Параметр	Описание	Тип	Настройка
Зона работы	Область, в которой детектируется наличие автомобиля	Обязательный	Разметка

Рекомендуемые разрешения видеопотоков для видеоаналитики

Для работы большинства детекторов не требуется HD поток. Чтобы сэкономить ресурсы сервера, рекомендуется заводить на камере отдельный облегчённый видеопоток для использования в видеоаналитических детекторах.

Рекомендуемые характеристики потоков для видеоаналитики:

- алгоритм сжатия: H.264;
- разрешение: см. таблицу ниже;
- FPS: от 5 до 7;
- GOP: до 15 (I-кадр не реже, чем в 2 сек.);
- битрейт: до 5 Мбит/с;
- CBR (Constant bitrate) — желательно.

Для снижения нагрузки на CPU выбирайте поток с меньшим разрешением (не ниже поддерживаемого детектором), низким FPS и алгоритмом сжатия H.264.

Название детектора	Рекомендуемое разрешение видеопотока
Распознавание гос. номеров машин	1920×1080
Толпа	640×360
Распознавание лиц	960×540
Падение человека	960×540
Огонь	640×360
Люди в запрещённой зоне	640×360
Движение людей в запрещённом направлении	640×360
Распознавание пола, возраста, эмоций	960×540
Каски	960×540
Подсчет людей	640×360
Очереди	640×360
Вмешательство в работу камеры	960×540
Движение в области кадра	960×540

Просмотр списка детекторов и нейросерверов

В разделе **Управление → Камеры → Детекторы** вы можете просмотреть список настроенных детекторов и управлять оптимизацией нейросерверов.

Список детекторов

Во вкладке **Детекторы** представлен список всех настроенных в системе детекторов. Выбор детектора производится из раскрывающегося списка в верхней части экрана.

Для каждого детектора отображается:

- название камеры и её IP-адрес;
- тип детектора;
- используемый видеопоток и его параметры;
- адрес модуля Spot, на котором работает детектор;
- текущий статус работы детектора;
- FPS;
- количество перезапусков с момента последнего запуска;
- дата и время последнего запуска;
- среднее время непрерывной работы;

- тип вычислительного устройства — CPU или GPU.

Нажав на название камеры, вы можете перейти в настройки камеры, вкладка **Видеоаналитика**.

Нейросерверы

Во вкладке **Нейросерверы** представлен список нейросерверов, задействованных в настроенных детекторах. Один нейросервер может использоваться несколькими детекторами одновременно. Один детектор может использовать несколько нейросерверов.

Для каждого нейросервера отображается:

- название нейросервера;
- статус оптимизации:
 - *Не оптимизирован* — оптимизация нейросервера ещё не проводилась;
 - *Ожидает оптимизации* — нейросервер находится в очереди на оптимизацию;
 - *Идёт оптимизация* — оптимизация выполняется в данный момент;
 - *Оптимизирован* — оптимизация успешно завершена;
 - *Ошибка оптимизации* — в процессе оптимизации возникла ошибка;
 - *Оптимизация прервана* — оптимизация была остановлена вручную
- дата последней попытки оптимизации;
- видеокарта, на которой работает нейросервер;
- размер батча обработки — количество кадров, которые нейросервер обрабатывает одновременно;
- модуль Spot, на котором расположен нейросервер;
- перечень детекторов, использующих данный нейросервер.

Управление оптимизацией

Оптимизация позволяет экономить ресурсы сервера и улучшить производительность детекторов, работающих на видеокартах NVIDIA. Процедуру рекомендуется выполнять в следующих случаях:

- при первичной настройке детекторов в системе;
- после обновления программного обеспечения;
- после изменения аппаратной конфигурации сервера;
- после обновления драйверов видеокарты.

Оптимизация нейросерверов проходит последовательно. На время оптимизации все детекторы останавливаются. После её завершения система автоматически перезапускает те детекторы, которые были запущены до начала оптимизации.

Кнопка **Управление оптимизацией** позволяет действия с нейросерверами:

- **Оптимизировать новые** — будут оптимизированы только нейросерверы в статусах «Не оптимизирован», «Ошибка оптимизации» или «Оптимизация прервана». В скобках указано количество таких нейросерверов. После завершения оптимизации система автоматически перезапустит детекторы, которые были запущены до её начала.
- **Оптимизировать все** — будут оптимизированы все нейросерверы вне зависимости от их текущего статуса. В скобках указано общее количество нейросерверов. Используйте этот вариант после обновления ПО, драйверов видеокарты или изменения аппаратной конфигурации. После завершения оптимизации система автоматически перезапустит детекторы, которые были запущены до её начала.
- **Отменить оптимизацию** — выполнить откат для всех ранее оптимизированных нейросерверов. После отмены оптимизации нейросерверам присваивается статус «Не оптимизирован».

Вы также можете выбрать действие отдельно для каждого нейросервера, нажав на три точки в правой части строки списка нейросерверов. Доступны следующие действия:

- оптимизировать первично или повторно;
- прервать оптимизацию;
- откатить.

Первичная оптимизация нейросервера

Действие **Оптимизировать** Запускает оптимизацию только тех нейросерверов, которые ещё не были оптимизированы (статус отличается от «Оптимизирован»).

Рекомендуется выполнять первичную оптимизацию при первичной настройке системы или если часть нейросерверов не прошла оптимизацию.

По завершении детекторы будут перезапущены автоматически.

Повторная оптимизация нейросервера

Повторная оптимизация доступна для нейросерверов, которые уже были оптимизированы ранее.

Рекомендуется выполнять повторную оптимизацию после обновления ПО, обновления драйверов или изменения аппаратной конфигурации.

По завершении детекторы будут перезапущены автоматически.

Прерывание оптимизации

Прерывание оптимизации доступно для нейросерверов в статусе «Идет оптимизация». Действие останавливает текущий процесс оптимизации.

После прерывания детекторы не запускаются автоматически. Нейросерверам, оптимизация которых была прервана, присваивается статус «Оптимизация прервана». Для возобновления работы запустите оптимизацию повторно, а затем вручную запустите нужные детекторы.

Откат оптимизации

Откат оптимизации отменяет результаты оптимизации для выбранного нейросервера и возвращает его в состояние до оптимизации.

Откат используется, если после оптимизации конкретный нейросервер работает некорректно.

Действие доступно только для нейросерверов со статусом «Оптимизирован». В случае неудачи нейросервер сохраняет статус «Оптимизирован» и на экране отображается сообщение об ошибке. При успешном откате нейросерверу присваивается статус «Не оптимизирован».

Особенности работы с несколькими модулями Spot

Если в системе используется несколько модулей Spot, оптимизация на каждом из них выполняется независимо. Нейросерверы, расположенные на разных Spot, оптимизируются параллельно, однако на каждом отдельном Spot в один момент времени оптимизируется не более одного нейросервера.

Интеграции с внешними системами

В Insentry доступны функции автоматизированного сбора информации об инцидентах безопасности от систем охранной, пожарной сигнализаций, СКУД, досмотрового оборудования и иных программных и аппаратных средств, интегрированных в системы безопасности предприятий. Эти данные передаются в ПО Insentry для обработки, хранения, анализа и представления в удобном для пользователя виде.

Интеграция со СКУД, пожарной и охранной сигнализацией доступна во всех платных редакциях.

Поддерживается интеграция со следующими системами:

- СКУД:
 - Рубеж;
 - RusGuard;
- пожарная сигнализация:
 - Modbus;
 - Рубеж;
 - Сфера;
 - Болид;
- охранный сигнализация:
 - Рубеж;
 - Сфера;
 - Болид.

Для настройки интеграции необходим модуль Get, который входит в базовый комплект поставки.

Подключение новых интеграций

Чтобы добавить новую интеграцию:

1. Перейдите в раздел **Управление → Устройства → Интеграции**.
2. Нажмите кнопку **Добавить**.
3. Выберите модуль Get, который будет использоваться для настройки интеграции.
4. Выберите тип интеграции.

Дальнейшая настройка зависит от внешней системы, с которой настраивается интеграция.

Интеграция с системой Болид

Для настройки интеграции с системой Болид укажите следующие параметры подключения:

- **Название** — название интеграции в Insentry;
- **Хост подключения** — адрес внешнего сервера, где находится интеграция;
- **Порт подключения** — порт подключения к внешнему серверу;
- **Использовать режим с авторизацией** — выбор режима подключения;
- логин и пароль для подключения к системе, с которой настраивается интеграция.

Интеграция с системой Сфера

Для настройки интеграции с системой Сфера укажите следующие параметры подключения:

- **Название** — название интеграции в Insentry;
- **Идентификатор клиента** — 160;
- **Идентификатор станции** — номер станции;
- **Хост подключения** и **Порт подключения** — адрес и порт подключения к внешнему серверу, к которому подключена система безопасности;
- **Входной IP** и **Входной порт** — адрес и порт локального сервера, на котором настраивается интеграция;
- **Исходящий IP** — 0.0.0.0;
- **Исходящий порт** — 15524;
- **Тип события по умолчанию**;
- **Использовать новое API Сфера 4500** — выбор API для обмена сообщениями.

Интеграция с системой RusGuard

Для настройки интеграции с системой RusGuard укажите следующие параметры подключения:

- **Название** — название интеграции в Insentry;
- **Хост подключения** — адрес внешнего сервера, где находится интеграция;
- **логин и пароль для подключения к системе**, с которой настраивается интеграция; **Тип события по умолчанию**.

Интеграция через плагин Insentry

Плагин Insentry позволяет подключить кастомные интеграции.

Для настройки интеграции с использованием плагина Insentry укажите следующие параметры подключения:

- **Название** — название интеграции в Insentry;
- **Хост подключения** — адрес внешнего сервера, где находится интеграция;
- **Порт подключения** — порт подключения к внешнему серверу;
- **Порт подключения к mqtt** — порт MessageBroker на внешнем сервере для обмена сообщениями;
- **логин и пароль для подключения к системе**, с которой настраивается интеграция.

Список интегрированных систем

Список систем, с которыми настроена интеграция, представлен в разделе **Управление → Устройства → Интеграции**.

По каждой системе представлена следующая информация:

- название системы;
- провайдер (название плагина);
- состояние;
- количество устройств: чёрным цветом отображаются добавленные в Insentry устройства; цифра на зелёном фоне — количество доступных устройств; цифра на красном фоне — количество недоступных устройств;
- используемый модуль Get;
- расположение (если указано);
- сервер.

Доступен поиск по названию внешней системы или плагина.

Сортировать таблицу можно по значению любого из столбцов. Для настройки сортировки кликните на название столбца. Стрелка у названия столбца показывает направление сортировки. При повторном клике на название столбца, по которому уже настроена сортировка, меняет направление сортировки.

При клике на название системы открывается карточка системы:

- вкладка **Датчики** — список датчиков, полученных из этой системы;
- вкладка **Настройки** — настройки интеграции.

Список датчиков

Внешние системы предоставляют Insentry информацию о датчиках, которые были в них добавлены. Датчики возможно разместить на картах, приписать им теги и выполнить иные настройки, доступные для устройств в Insentry.

Датчики из внешних систем могут быть удалены встроенными средствами этих систем, при этом автоматического удаления датчика из Insentry не происходит. Чтобы избежать ситуации, когда данные от датчика временно перестают приходить, и датчик при этом автоматически удаляется, удалить датчик из Insentry можно только вручную по решению администратора.

По каждому датчику отображается информация:

- название — чёрным цветом отображаются датчики, добавленные в Insentry, зелёным — доступные для добавления датчики; красным — датчики, от которых перестали приходить данные;
- вендор/модель;
- расположение (если задано);
- зона (если получена информация о принадлежности датчика зоне);
- иконка для перехода к просмотру расположения датчика на карте;
- доступность. Индикатор показывает статус доступности датчика в Insentry:
 -  — датчик работает правильно;
 -  — состояние датчика неизвестно;
 -  — датчик в состоянии сбоя;
 -  — связанный с датчиком плагин Get недоступен. Нет данных о состоянии подключения к внешней системе и состоянии датчика.

Таблицу можно отсортировать по столбцам **Название** и **Вендор/модель**. Для настройки сортировки кликните на название столбца. Стрелка у названия столбца показывает направление сортировки. При повторном клике на название столбца, по которому уже настроена сортировка, меняет направление сортировки.

Доступен поиск по названию устройства. Обратите внимание, что в поисковой строке название должно быть указано полностью. По вхождению введённых символов в название поиск не будет выполнен.

Также доступен расширенный режим поиска.

Настройки интеграции

Во вкладке **Настройки** вы можете изменить настройки интеграции с внешней системой:

- название;
- расположение;
- хост подключения;
- порт подключения;

- логин;
- пароль.

Список полей зависит от типа интегрированной системы.

В фильтре событий показаны типы событий, полученные по API из внешней системы. Если во внешней системе есть события, настроенные вручную, их необходимо настроить при помощи кнопки **Добавить значение**.

Чтобы не получать в Insentry информацию по определённому событию, удалите событие из списка.

Реестр устройств

В разделе **Управление → Интеграции → Реестр устройств** отображается полный список устройств, полученных от всех интегрированных внешних систем.

Датчики

Настройки

Датчики

Введите ваш запрос

Включить расширенный поиск

☐	Название ↓	Вендор / Модель ↓	Расположение	Зона	На карте	Доступность
☐	 АМ-40 1.2.1.2	rubezh				Удалить
☐	 АМ-40 1.2.1.2	rubezh		Архив		Добавить
☐	 ИО 40920-2 1.2.1.6	rubezh				Удалить
☐	 ИО 40920-2 1.2.1.6	rubezh		Офис		Добавить
☐	 Реле 1.2.1	rubezh				Удалить
☐	 Реле 1.2.2	rubezh				Удалить
☐	 Реле 1.2.3	rubezh				Удалить
☐	 Реле 1.2.1	rubezh				Добавить
☐	 Реле 1.2.2	rubezh				Добавить

По каждому датчику отображается информация:

- название — чёрным цветом отображаются датчики, добавленные в Insentry, зелёным — доступные для добавления датчики; красным — датчики, от которых перестали приходить данные;
- вендор/модель;
- расположение (если задано);
- зона (если получена информация о принадлежности датчика зоне);
- иконка для перехода к просмотру расположения датчика на карте;
- доступность. Индикатор показывает статус доступности датчика в Insentry:
 -  — датчик работает правильно
 -  — состояние датчика неизвестно;
 -  — датчик в состоянии сбоя;
 -  — связанный с датчиком плагин Get недоступен. Нет данных о состоянии подключения к внешней системе и состоянии датчика.

Красным в списке обозначены датчики, если связанный с датчиком плагин Get онлайн и у него есть активное подключение к внешней системе, которая сообщает, что датчик в состоянии сбоя.

Доступные во внешней системе датчики можно добавить в Insentry, недоступные — удалить из списка. Если датчик снова выйдет на связь, он появится в списке и его можно будет снова добавить в Insentry.

Таблицу можно отсортировать по столбцам **Название** и **Вендор/модель**. Для настройки сортировки кликните на название столбца. Стрелка у названия столбца показывает направление сортировки. При повторном клике на название столбца, по которому уже настроена сортировка, меняет направление сортировки.

Доступен поиск по названию устройства. Обратите внимание, что в поисковой строке название должно быть указано полностью. По вхождению введённых символов в название поиск не будет выполнен.

Также доступен расширенный режим поиска.

При клике на строку таблицы реестра устройств открывается карточка устройства.

Карточка датчика

Карточка датчика содержит вкладки:

- **Настройки** — информация по датчику;
- **Права** — настройка прав доступа пользователей к управлению датчиком — аналогично [настройке прав доступа на камеру](#)
- **Связанные объекты** — настройка связи с другими устройствами, информация с которых может быть полезна при обработке событий, полученных с выбранной камеры;
- **Теги** — [присвоение тегов](#).

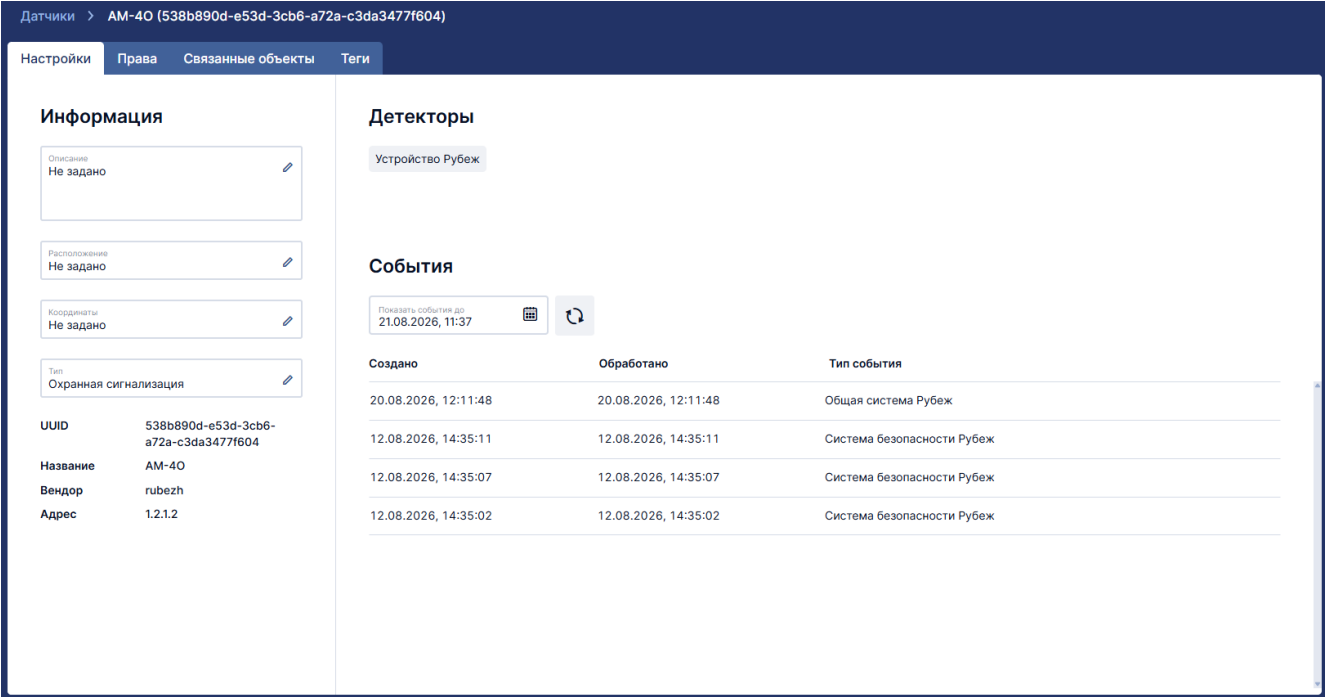
Настройки датчика

Во вкладке **Настройки** в карточке датчика отображаются поля:

- **Описание** — произвольное описание датчика в Insentry;
- **Расположение** — выбор расположения из [справочника тегов и расположений](#);
- **Координаты** — географические координаты расположения датчика. Если заданы, датчик будет отображаться на карте в разделе **Карты**;
- **Тип** — тип датчика;
- **UUID** — уникальный идентификатор датчика;
- **Название** — название датчика в системе безопасности;
- **Вендор** — производитель датчика;
- **Адрес** — адрес датчика во внешней системе.

В разделе **Детекторы** показаны детекторы системы сигнализации, по которым возможны тревоги с выбранного датчика.

В разделе **События** показаны события от выбранного датчика и связанных устройств (если настроена нисходящая связь от этого детектора к другим устройствам).



Права доступа к информации с датчика

Для доступа к событиям от датчика у пользователя должны быть права уровня «Наблюдение» и «Архив».

Связанные объекты

Связи с другими объектами настраиваются аналогично тому, как это делается на камере.
См. [Настройка связанных устройств на камере](#).

Теги

Теги присваиваются датчикам так же, как камерам, и помогают фильтровать список устройств.
См. [Присвоение тегов на камере](#)

Зоны

В разделе **Управление → Устройства → Интеграции → Зоны** показан список зон (охранных, пожарных и др.), полученных от интегрированных внешних систем.

Зоны					
Название	Система безопасности	Сервер	Устройства	На охране	
Архив	рубеж		1	✕	Поставить на охрану
Бухгалтерия	рубеж		1	✓	Снять с охраны
Офис	рубеж		1	✕	Поставить на охрану

По каждой зоне отображается:

- название;
- система безопасности, которой принадлежит выбранная зона. При клике на название системы безопасности открываются настройки системы безопасности в разделе **Интеграции**;
- количество устройств в зоне;
- статус активности (поставлена на охрану / снята с охраны) — отображается только для охранных зон;
- кнопка изменения статуса активности зоны — отображается только для охранных зон.

Список зон имеет древовидную структуру — зоны могут быть вложены друг в друга.

При клике на строку таблицы открывается карточка зоны:

- вкладка **Датчики** — список датчиков в выбранной зоне;
- вкладка **Настройки** — настройки зоны:
 - статус активности зоны с возможностью изменения (только для охранных зон);
 - название системы безопасности, которой принадлежит выбранная зона. При клике на название системы безопасности открываются настройки системы безопасности в разделе **Интеграции**;
 - идентификатор зоны во внешней системе;
 - описание.

Зону можно поставить на охрану или снять с охраны с помощью кнопки в правой части строки таблицы зон, из настроек конкретной зоны либо из карточки инцидента (для зон системы Рубеж).

Карты

В разделе **Управление → Карты** можно отметить расположение камер и датчиков на карте или схеме здания. Карты и схемы загружаются из произвольных [источников](#).

Карты

Слои

Карты

Добавить

Название ↓	Статус	Размер	Масштаб, от	Масштаб, до	Формат	Прокси
vest	Загружена	77 МБ	2	7	PBF	Нет
Карта мира	Загружена	69 МБ	1	7	PNG	Нет

Устройства могут располагаться:

- на карте — в этом случае их расположение задано [координатами в настройках](#);
- внутри зданий — в этом случае устройства привязываются к [плану этажа](#) и отображаются на карте только в том случае, если на ней отображается соответствующий этаж.

Добавление новой карты

Карты можно загрузить с тайлового сервера Insentry либо из произвольного источника.

Перейдите в раздел **Управление → Карты** и нажмите кнопку **Добавить**. Откроется окно добавления карт из произвольных источников.

Чтобы добавить карту:

1. В поле **Источник** укажите [источник](#) для загрузки карты. Чтобы добавить карту с тайлового сервера Insentry, выберите здесь Insentry Cloud Map.
2. Укажите название карты.
3. В поле **Привязка к слою** укажите один или несколько [слоёв](#), в которые будет включена карта. Слои позволяют просматривать на одной карте несколько областей в нужном масштабе.

Новая карта

+

−

Текущий масштаб

6

Источники

1

Название карты*

Привязка к слою

Не выбрано

Прокси

Масштабы карты

Светлый квадрат — область, которая будет скачана, в мин. масштабе. Двигайте карту так, чтобы ваш объект находился внутри квадрата. Карта будет скачана слоями в масштабах от минимального до максимального.

Зафиксировать область

Мин. масштаб

6

Макс. масштаб

7

Размер

Карта займёт от 2 до 3 МБ

Отмена

Скачать

Вы можете предварительно [создать слой](#) в разделе **Управление → Карты → Слои** и включить в них загружаемую карту.

Карты в слое накладываются друг на друга в порядке загрузки, и «верхней» будет наложена последняя загруженная карта. Учитывайте это при включении карты в слой.

4. Переключатель **Прокси** позволяет проксировать карту при запросах тайлов без клонирования в хранилище. Если параметр отключен, то выбранный участок карты клонируется во внутреннее хранилище, и в процессе клонирования карта уже доступна для просмотра.

5. Задайте минимальный и максимальный масштабы карты для скачивания. Разница между масштабами определяет количество слоёв карты, которые будут скачаны. Слои дают возможность приближать карту. Чем больше разница между минимальным и максимальным масштабом, тем больше места на диске займёт карта после скачивания.

Светлый квадрат на карте обозначает границы карты в минимальном масштабе. Двигайте карту так, чтобы интересующая вас область находилась внутри квадрата. Центр квадрата совпадает с центром видимой области карты. Проверить отображение карты в нужном масштабе можно при помощи переключателя **Масштаб** в правом верхнем углу карты.

Переключатель **Зафиксировать область** позволяет ограничить скачиваемую область выбранным минимальным масштабом и не двигать её при зуме и сдвиге карты.

Чтобы не допускать отсутствие тайлов при скроле карты от самого малого масштаба до указанного в поле **Минимальный масштаб**, при загрузке карты дополнительно скачиваются несколько тайлов вокруг области внутри квадрата. Это существенно снижает объём загруженных данных, так как загружается не вся карта целиком в пропущенных масштабах, а только несколько тайлов.

6. Нажмите кнопку **Скачать**. Начнётся скачивание карты из указанного источника. Время скачивания зависит от самой карты и от выбранного масштаба.

Слои

Карты привязываются к слоям. Слои позволяют просматривать одновременно несколько карт в нужном масштабе.

Слой содержит карты, скачанные с сервера Insentry (по умолчанию) или из произвольного источника (если, к примеру, вам нужна топографическая карта мира). Можно также добавить в слой другие карты, например, карты районов, где расположены объекты видеонаблюдения, и планы строений. Таким образом, при просмотре слоя в разделе **Карты** оператор увидит наложенные друг на друга карты и планы, привязанные к выбранному слою.

Карта может быть привязана к нескольким слоям. Слой может содержать только карты одного типа — векторные либо растровые. Добавить в один слой карты разных типов не получится. Тип слоя определяется по первой добавленной в него карте.

Карты в слое накладываются друг на друга в порядке загрузки, и «верхней» будет наложена последняя загруженная карта. Учитывайте это при включении карты в слой.

Создание слоя и привязка карт к слою

В разделе **Управление → Карты → Слои** можно создавать новые слои, задав для них название. Карты добавляются в слои на основании того, какие слои отмечены в поле **Привязка к слою** в настройках карты при скачивании.

Редактирование привязки карты к слою

Удалить карту из слоя можно при редактировании карты, сняв отметку с нужного слоя, или в настройках слоя, нажав кнопку удаления в списке карт слоя. Если карта не привязана ни к одному из слоёв, она не будет отображаться при просмотре в разделе **Карты**.

Привязать карту к другому слою можно в окне редактирования карты в разделе **Управление → Карты**.

Примеры настройки слоёв

Слой	Карты	Планы
Мои объекты	Карты районов или городов, где размещены объекты	Планы строений
Центральный офис	Карта города, карта района	Планы строений
Дача	Карта района или улицы	Планы построек на участке

Добавление источника карт или схем

По умолчанию в Insentry доступен источник Insentry Cloud Map — это карта мира Open Street Map, которую можно скачать с сервера Insentry. Вы можете добавить другие источники для загрузки тайловых карт и интерактивных планов зданий.

Чтобы добавить новый источник:

1. В разделе **Управление → Карты** перейдите на вкладку **Источники** и нажмите кнопку **Добавить**.
2. Укажите подложку и название нового источника.
3. Выберите схему, которая будет использована при загрузке тайлов: http, https или file. От выбранной схемы зависит шаблон адреса для загрузки тайлов.
4. Укажите шаблон URL или URI для выбранной схемы.

Шаблон URL для http/https: `127.0.0.1:8000/tile/{Z}/{X}/{Y}.png` . Порт указывать не обязательно. Плейсхолдер {P} для префиксов не обязательный. Если нужно, он указывается перед IP или доменным именем:

`http://{P}.127.0.0.1:8000/tile/{Z}/{X}/{Y}.png` . Если указан плейсхолдер {P}, префиксы нужно задать в отдельном поле **Префиксы**, указав нужные префиксы через пробел. Если префиксы не используются, оставьте это поле пустым.

Шаблон URI для схемы file: `C:/maps/{Z}/{X}/{Y}.png` для Windows или `mnt/map/{Z}/{X}/{Y}.png` для Linux. Поддерживаются файлы форматов .pdf, .png, *.pbk.

5. Нажмите кнопку **Сохранить**. После сохранения источник появится в списке источников и вы сможете скачать карту или план строения из этого источника.

Строения

Строения позволяют указать точное расположение устройств внутри здания.

В Insentry для строения можно указать следующие данные:

- широта и долгота — можно ввести вручную или отметить расположение на карте;
- тег расположения — объединить с помощью тега строение с устройствами, расположенными внутри него;
- этажи — для каждого этажа можно указать свой план и отметить на нём расположение устройств.

Этажи

Чтобы добавить этаж, укажите его название, высоту и тег расположения (не обязательно).

Высота условно обозначает уровень этажа в строении и позволяет расположить этажи в нужном порядке.

Планы

После того, как для строения задан хотя бы один этаж, можно загрузить его план и расположить на плане устройства.

Строения > str1

Планы Этажи Настройки

Планы

Название ↑	Тип	Статус	Размер	Масштаб, от	Масштаб, до	Формат	Прокси
этаж 1							
1	Графический	Загружен	172 МБ	0	7	PNG	Нет
2	Графический	Загружен	29 МБ	0	7	PNG	Нет
1	Интерактивный	Загружен	8 МБ	16	22	PBF	Нет

[↓ Добавить графический план](#)
[↓ Добавить интерактивный план](#)

[+ Добавить этаж](#)

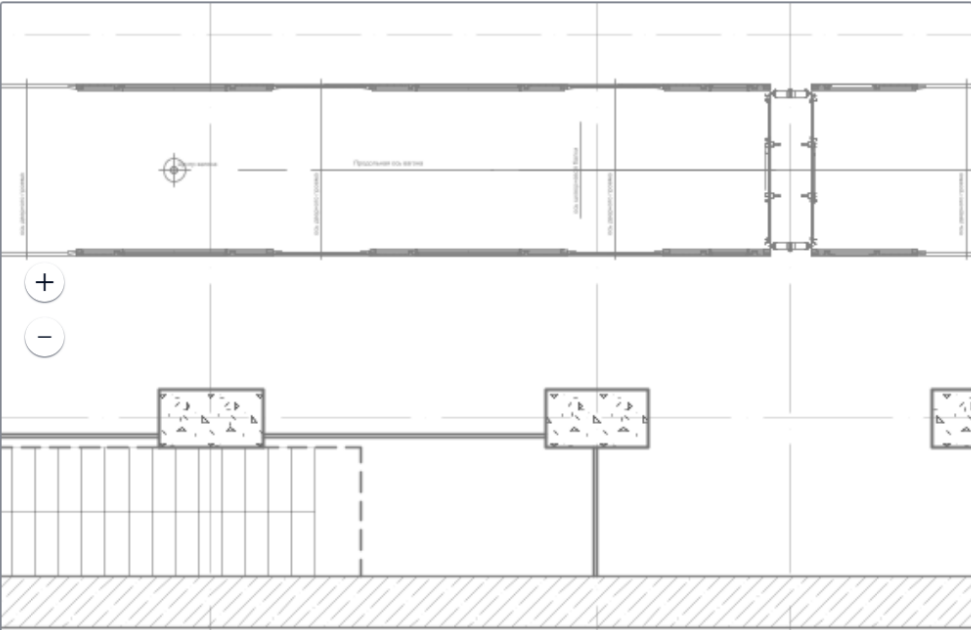
В Insentry поддерживаются планы двух типов:

- графический план — растровое изображение в формате *.pdf. Графические планы загружаются из файла и поддерживают приближение/отдаление. Отображаются в отдельном окне поверх открытой карты.
- интерактивный план — загружается из векторных источников подобно тайловым картам. Интерактивный план показан прямо на карте, вращается вместе с картой и масштабируется в рамках доступного диапазона масштабов.

Чтобы указать расположение графического плана на карте, нажмите кнопку  в правой части строки нужного плана в списке планов и укажите точные координаты расположения здания либо отметьте место на карте.

Расположение интерактивного плана определяется согласно источнику.

Новый графический план



Название*
Этаж 1

Этаж
1

vector_pdf.pdf
Допустимые форматы: PDF

Загрузить

Отменить Сохранить

Новый интерактивный план



Название*
Кунцево

Источник
peres

Мин. масштаб
18

Макс. масштаб
22

☐ Прокси

Размер ⓘ
Карта займёт от 24 до 36 МБ

Отменить Сохранить

Переключатель **Прокси** позволяет проксировать карту при запросах тайлов без клонирования в хранилище. Если параметр отключен, то выбранный участок карты клонируется во внутреннее хранилище, и в процессе клонирования карта уже доступна для просмотра.

Настройки строения

Во вкладке **Настройки** вы можете:

- изменить название строения,
- [выбрать из справочника](#) тег расположения строения;

- задать координаты расположения строения на карте. Если координаты заданы, то устройства, расположенные в выбранном строении, будут отображаться на карте в разделе **Просмотр**.

Объекты

В разделе **Управление** → **Карты** → **Объекты** можно задать расположение устройств на карте или плане строения.

Добавление объекта на карту

Чтобы добавить объект на карту:

1. В правой части экрана выберите тип устройства.
2. Выделите устройство в списке. Выбранное устройство будет отмечено рамкой.
3. Кликните в место на карте или плане, куда вы хотите поместить устройство.

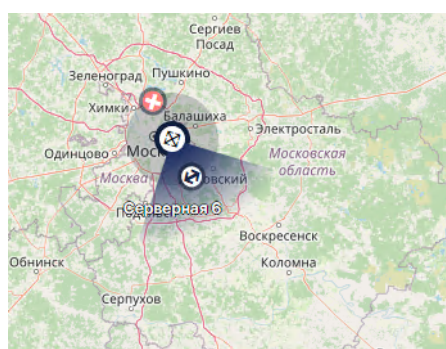
Чтобы расположить устройство на плане этажа, кликните левой кнопкой мыши на значок строения на карте и в выпадающем списке выберите нужный этаж. Расположить камеру на графическом плане возможно только если указаны координаты строения (в настройках строения) и плана.

Указать расположение камеры на карте можно также в [настройках камеры](#) — указав ширину и долготу местонахождения карты в поле **Координаты**.

Настройка расположения и угла обзора камеры

Когда камера размещена на карте, вы можете изменить её расположение и угол обзора. Для этого кликните на значок камеры.

Появятся элементы управления:



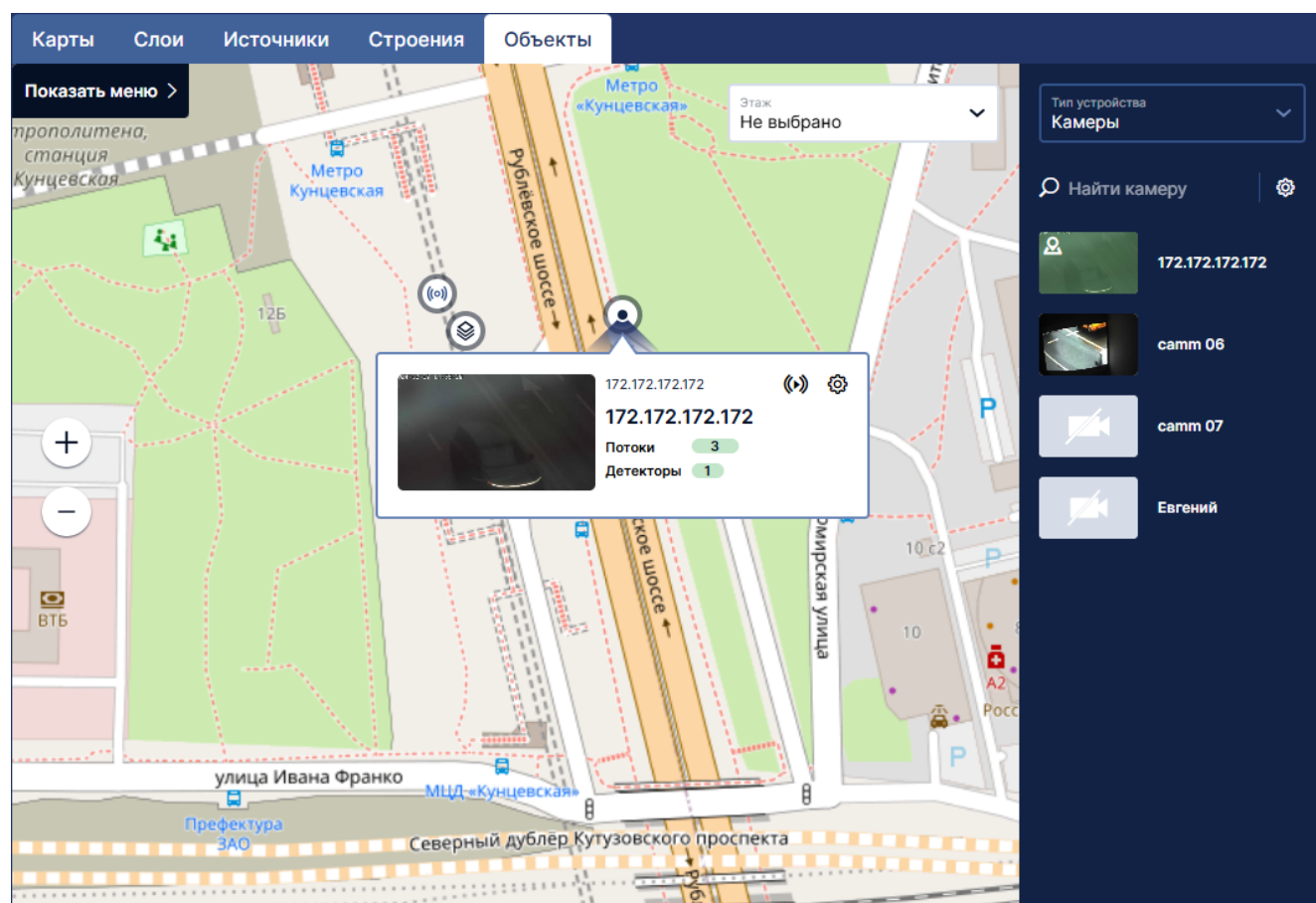
Чтобы изменения вступили в силу, нажмите на любое место на карте вне виджета камеры.

Просмотр объектов на карте

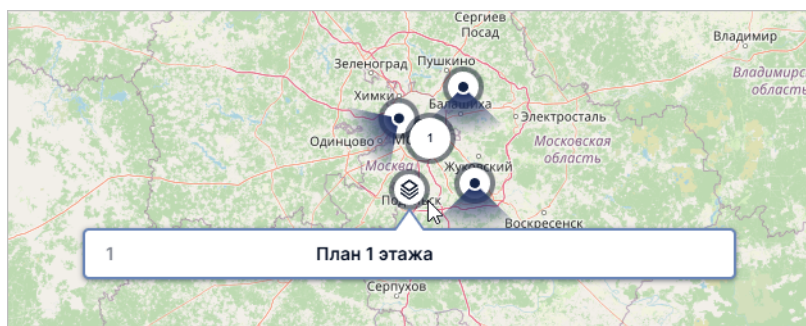
Условные обозначения объектов на карте:

	Строение
	Отдельный план этажа
	Группа объектов. Приблизьте карту, чтобы увидеть их по отдельности
	Датчик
	Камера

При наведении курсора на значок камеры отображается информация о потоках и кнопки для перехода к просмотру живого видео и настройкам камеры. Цветные обозначения камер и потоков такие же, как в списке камер.



По клику на значок строения открывается список планов этажей, если планы были загружены в настройках строения.



По клику на план открывается план строения, на котором можно расположить устройства так же, как на карте. Расположить устройства на плане этажа можно только если указано расположение всего строения либо плана этажа.

По нажатию кнопки **Показать меню** в левой части экрана открывается меню, где можно:

- выбрать слой для отображения;
- включить или отключить отображение названий объектов на карте;
- центрировать карту по расположению строения (если задано).

Чтобы при приближении карты отображался интерактивный план:

- масштаб плана должен совпадать с масштабом карты;
- центр просматриваемого участка карты должен попадать в границы плана.

Чтобы повернуть карту, нажмите Ctrl и вращайте карту, удерживая ЛКМ. На векторных картах и планах отображается значок компаса в правой части экрана. Стрелкой отмечено направление на север. При клике в центр «компаса» карта возвращается к стандартному виду (сервер — сверху).

Справочники

Email уведомления

Уведомления отправляются на электронную почту пользователей при наступлении событий, зафиксированных детекторами.

Для настройки отправки уведомлений по электронной почте:

1. Создайте пароль для внешнего приложения в почтовой службе, которую вы используете.
[Пароль приложения в Mail.ru](#) [Пароль приложения в Яндексе](#)
2. Откройте файл конфигурации application.properties модуля Watch.

Расположение файла конфигурации модуля Watch при установке в папку по умолчанию: Linux: /usr/src/InSentry/Watch/application.properties Windows: C:\Program Files\InSentry\Watch.Lite\application.properties

3. Укажите следующие параметры:

```
spring.profiles.active=mailing
mailsender.hostname=[адрес сервера исходящей почты]
mailsender.protocol=smtp
mailsender.port=587
mailsender.user=[почта отправителя]
mailsender.password=[пароль приложения]
```



```

mailsender.mail.smtp.auth=true
mailsender.mail.smtp.starttls.enable=true
mailsender.mail.debug=true
mailsender.mail.recipients=[адреса почты получателей уведомлений через запятую]
mailsender.mail.license.admin.email=[адрес почты администратора]

```

4. Сохраните и закройте файл конфигурации.
5. Когда конфигурация указана, настроить и проверить отправку уведомлений по событиям определённых детекторов можно в разделе **Управление → Справочники → Уведомления**. Если уведомления не приходят, перезапустите службу Insentry.Watch.

Расписания

Расписание используется для настройки записи архива и других функций Insentry по заданному графику. Чтобы указать расписание при настройке детекторов, уведомлений, архива, расписание должно быть предварительно создано и настроено.

Расписание состоит из одного или нескольких интервалов работы.

Поддерживаются интервалы двух типов:

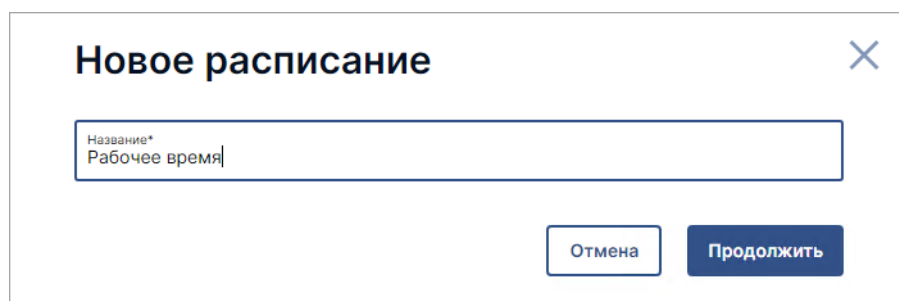
- ежедневные — интервал задаётся только временем начала и окончания и повторяется каждый день;
- еженедельные — интервал задаётся как непрерывный период от одного дня недели и времени до другого дня недели и времени. Допускаются интервалы, пересекающие границу суток: если время окончания меньше времени начала, интервал считается завершающимся на следующих сутках.

Расписания можно настроить в разделе **Управление → Справочники → Расписания**.

Создание расписания

Чтобы создать новое расписание:

1. В разделе **Управление → Справочники → Расписания** нажмите кнопку **Добавить расписание**.
2. Укажите название расписания. Для каждого расписания название должно быть уникальным (не совпадать с названием других расписаний в системе).



3. Нажмите **Продолжить**. Расписание будет сохранено, но не заполнено: чтобы в расписании появилось время работы, нужно добавить в него интервалы.

4. Нажмите **Добавить интервал**, чтобы добавить в расписание первый интервал.

Одно расписание может содержать несколько интервалов. Интервалы могут пересекаться.

5. Укажите значения параметров интервала в полях формы:

- **Периодичность**;
- **Начало и Конец** — дни работы;
- **Часы и Минуты** — начало и окончание периода работы в указанные дни.

Ежедневный интервал задаётся только временем начала и окончания и повторяется каждый день. Ежедневный интервал задаётся как непрерывный период от одного дня недели и времени начала до другого дня недели и времени окончания.

Если время окончания меньше времени начала, то время окончания будет назначено на следующие сутки. Например, интервал с 20:00 до 5:00 означает с 20 вечера текущего дня до 5 утра следующего дня.

1. Сохраните настройки. Будет представлен список расписаний. Новое расписание будет отображено в списке:

Просмотр списка расписаний

Перейдите в раздел **Управление → Справочники → Расписания**.

Расписания						Добавить расписание
Название	Статус	Периодичность	Уведомления	Детекторы	Архивы	
Рабочее время	Активен	Еженедельно, Понедельник - Пятница, 9:00 - 18:00		1	2	
Выходные и ночь	Неактивен	Еженедельно, Пятница - Понедельник, 18:00 - 9:00 Ежедневно, 20:00 - 7:00				  

В списке расписаний по каждому расписанию отображаются:

- **Название** — название расписания. Указывается при [создании](#);
- **Статус** — активен/неактивен. Если расписание нигде не используется — оно неактивно;
- **Периодичность** — интервалы работы расписания;
- **Уведомления** — количество уведомлений, в которых задействовано расписание;
- **Детекторы** — количество детекторов, в которых задействовано расписание;
- **Архивы** — количество правил записи архива, в которых задействовано расписание.

При наведении курсора на строку, доступны действия:

-  — копировать расписание (создать новое расписание с аналогичными настройками);
-  — редактировать параметры интервалов расписания (время, периодичность);
-  — удалить расписание.

При клике на название расписания, будет представлено окно его настроек со списком интервалов:

Расписания > Выходные и ночь

Интервалы
Уведомления

Интервалы

Добавить интервал

 Еженедельный	Пятница - Понедельник, 18:00 - 9:00	 
 Ежедневный	20:00 - 7:00	

При наведении курсора на строку, доступны действия с интервалом:

-  — редактировать параметры интервала (время, периодичность),
-  — удалить интервал из расписания.

Редактирование параметров расписания

- [Изменение названия расписания](#)
- [Изменение состава и настроек интервалов](#)

Перейдите в раздел **Управление → Справочники → Расписания**.

Расписания						Добавить расписание
Название	Статус	Периодичность	Уведомления	Детекторы	Архивы	
Рабочее время	Активен	Еженедельно, Понедельник - Пятница, 9:00 - 18:00		1	2	
Выходные и ночь	Неактивен	Еженедельно, Пятница - Понедельник, 18:00 - 9:00 Ежедневно, 20:00 - 7:00				  

В расписании можно редактировать:

1. название;
2. параметры: состав и настройки интервалов.

Изменение названия расписания

Наведите курсор на строку с расписанием и нажмите кнопку редактирования .

Переименовать расписание

Название*
Каждый день

Отмена
Сохранить

Укажите новое название расписания и нажмите кнопку **Сохранить**.

Изменение состава и настроек интервалов

Перейдите в раздел **Управление → Справочники → Расписания** и нажмите на название расписания в списке. Будет представлено окно его настроек со списком интервалов:

Расписания > Выходные и ночь

Интервалы
Уведомления

Интервалы

Добавить интервал

Еженедельный
Пятница - Понедельник, 18:00 - 9:00

Ежедневный
20:00 - 7:00

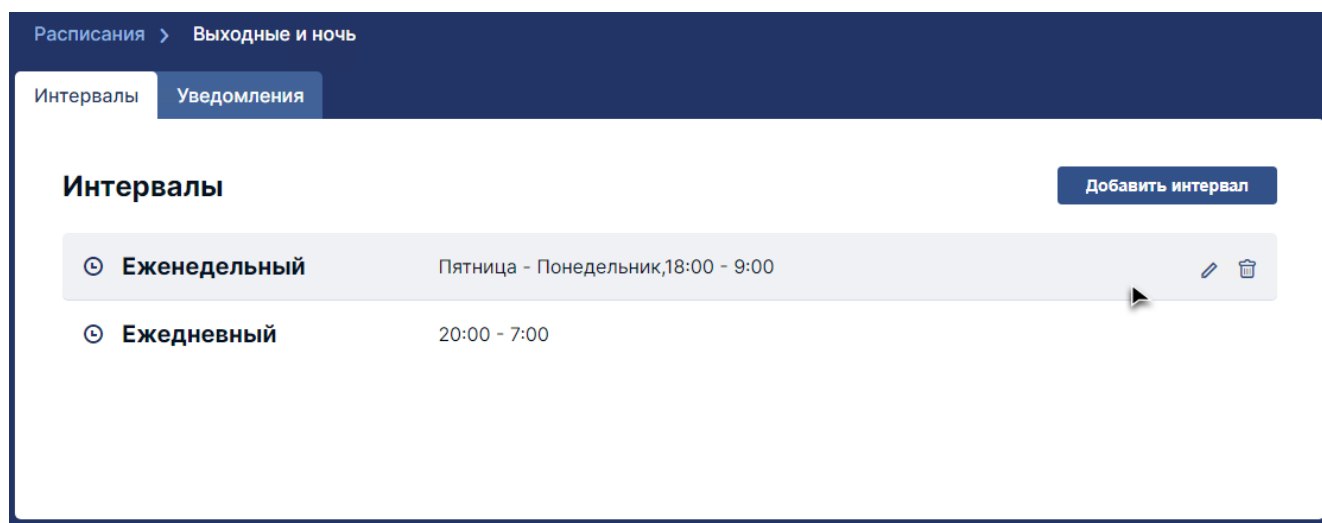
При наведении курсора на строку, доступны действия с интервалом:

-  — [редактировать параметры интервала](#) (время, периодичность),
-  — удалить интервал из расписания.

Настройка интервалов

- [Добавление интервала](#)
- [Изменение параметров интервала](#)
- [Удаление интервала](#)

Перейдите в раздел **Управление** → **Справочники** → **Расписания** и нажмите на название расписания в списке. Будет представлено окно его настроек со списком интервалов:



Добавление интервала

Добавить интервал

Периодичность

Ежедневный

▼

Часы

09

▼

:

Минуты

00

▼

-

Часы

18

▼

:

Минуты

00

▼

Отмена

Сохранить

Одно расписание может содержать несколько интервалов. Интервалы могут пересекаться.

Укажите значения параметров интервала в полях формы:

- **Периодичность**;
- **Начало и Конец** — дни работы;
- **Часы и Минуты** — начало и окончание периода работы в указанные дни.

Ежедневный интервал задаётся только временем начала и окончания и повторяется каждый день. Еженедельный интервал задаётся как непрерывный период от одного дня недели и времени начала до другого дня недели и времени окончания.

Если время окончания меньше времени начала, то время окончания будет назначено на следующие сутки. Например, интервал с 20:00 до 5:00 означает с 20 вечера текущего дня до 5 утра следующего дня.

Изменение параметров интервала

Наведите курсор на строку с описанием интервала и нажмите кнопку . Заполните поля аналогично тому, как это делается при создании интервала.

Удаление интервала

Наведите курсор на строку с описанием интервала и нажмите кнопку . Подтвердите удаление.

Удаление расписания

Расписание можно удалить только если оно не используется в системе. Такое расписание имеет статус «Неактивен». Проверить статус можно в списке расписаний.

Перейдите в раздел **Управление → Справочники → Расписания**.

Расписания						Добавить расписание
Название	Статус	Периодичность	Уведомления	Детекторы	Архивы	
Рабочее время	 Активен	Еженедельно, Понедельник - Пятница, 9:00 - 18:00		1	2	
Выходные и ночь	 Неактивен	Еженедельно, Пятница - Понедельник, 18:00 - 9:00 Ежедневно, 20:00 - 7:00				  

Наведите курсор на строку с расписанием, которое нужно удалить, и нажмите кнопку удаления .

Подтвердите операцию:



Удаление расписания

Вы уверены, что хотите удалить расписание Выходные и ночь ?

Отмена

Да, удалить

Транспорт

В разделе **Управление → Справочники → Транспорт** настраивается список номеров транспортных средств.

Список поможет найти фото и время события, когда транспортное средство с определённым номером проехало мимо камеры. Для этого на камере должен быть запущен [детектор автомобильных номеров](#).

Добавление транспортного средства

Чтобы добавить транспортное средство:

1. Перейдите в раздел **Управление → Справочники → Транспорт**.
2. Нажмите кнопку **Добавить**.
3. Укажите страну, в которой зарегистрировано транспортное средство.
4. Укажите регистрационный номер транспортного средства. Формат номера должен соответствовать выбранной стране.
5. Укажите описание транспортного средства, если нужно.
6. Нажмите кнопку **Сохранить**.

Новое транспортное средство

Страна
Россия

Регистрационный номер*
A123AA77
Формат: цифры, кириллица (А, В, Е, К, М, Н, О, Р, С, Т, У, Х) и латиница (С, D, Т). Без пробелов

Описание

Отмена

Сохранить

Список номеров транспортных средств

Список можно просмотреть в разделе **Управление → Справочники → Транспорт**.

Транспортные средства

Добавить

Искать по номеру или описанию

Регистрационный номер	Описание	Теги
E640AC16		
K854AE99		
M4480E67		
P942BO799		
C085KK77		
T571KX797		

Для каждого транспортного средства отображается номер, произвольное описание (если задано) и теги.

Поиск доступен по номеру или и содержимому поля **Описание**.

По клику на номер ТС в списке можно просмотреть список событий — фото и время, когда транспортное средство с этим номером проезжало мимо камеры, на которой запущен [детектор распознавания номеров транспортных средств](#).

События с транспортным средством

Чтобы найти события, когда транспорт с определённым номером проезжал мимо камеры, на которой запущен [детектор автомобильных номеров](#), выберите регистрационный номер в списке.

Информация

Регистрационный номер
A111YA 799

Описание ТС
As digital systems evolved and miniaturized, the simple turned complex...

Теги

Родительский тег / ... / тег

... / ... / Длинный вложенный тег

Еще один тег

+

События

Начало отрезка
15.05.2022

Конiec отрезка
25.05.2022

Камера
Выбрано: 5

Преды
Весь кадр



12:34:27, 25.09.2020
АТП29522



12:34:27, 25.09.2020
АТП29522



12:34:27, 25.09.2020
АТП29522



12:34:27, 25.09.2020
АТП29522



12:34:27, 25.09.2020
АТП29522



12:34:27, 25.09.2020
АТП29522



12:34:27, 25.09.2020
АТП29522

В левой части экрана будет представлена информация о транспортном средстве, её можно редактировать.

Если на камере запущен [детектор автомобильных номеров](#) и детектор распознал номер, то в разделе **События**, будут показаны кадры, на которых детектор распознал ТС с указанным номером. Во внутренней базе Insentry сохраняются номера всех проехавших ТС, пока детектор запущен. Поэтому как только номер добавлен в список, если транспортное средство с этим номером уже проезжало мимо камеры ранее, в списке событий это будет отображаться.

В верхней части раздела **События** возможно настроить отображение событий:

- начало и конец отрезка — показывать события только за определённый период времени;
- **Камеры** — выбрать, события с каких камер показывать;
- **Превью** — отображать на превью в списке событий весь кадр или только область с номером.

Люди

В разделе **Управление → Справочники → Люди** настраивается список лиц, который нужен для работы [детектора идентификации лиц](#).

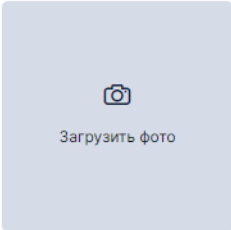
При распознавании лица детектор будет сравнивать изображение с фотографией человека из списка лиц. Заполнять список не обязательно — детектор может работать в режиме оповещения обо всех людях, в этом случае список можно оставить пустым.

Добавление новой персоны

Чтобы добавить человека в список, нажмите кнопку **Добавить** на экране списка персон (**Управление → Справочники → Люди**).

Новая карточка персоны

✕



Требования к файлу: jpeg, весом до 1.5 МБ

Отмена

Добавить

Укажите фамилию и имя человека.

Загрузите фото лица в формате jpeg. Размер файла не более 1,5 МБ. На фото должно быть хорошо видно лицо — по фото детектор определяет, похож ли проходящий мимо камеры человек на персону из списка.

Нажмите кнопку **Сохранить**.

Список персон

Список персон представлен в разделе **Управление → Справочники → Люди**.

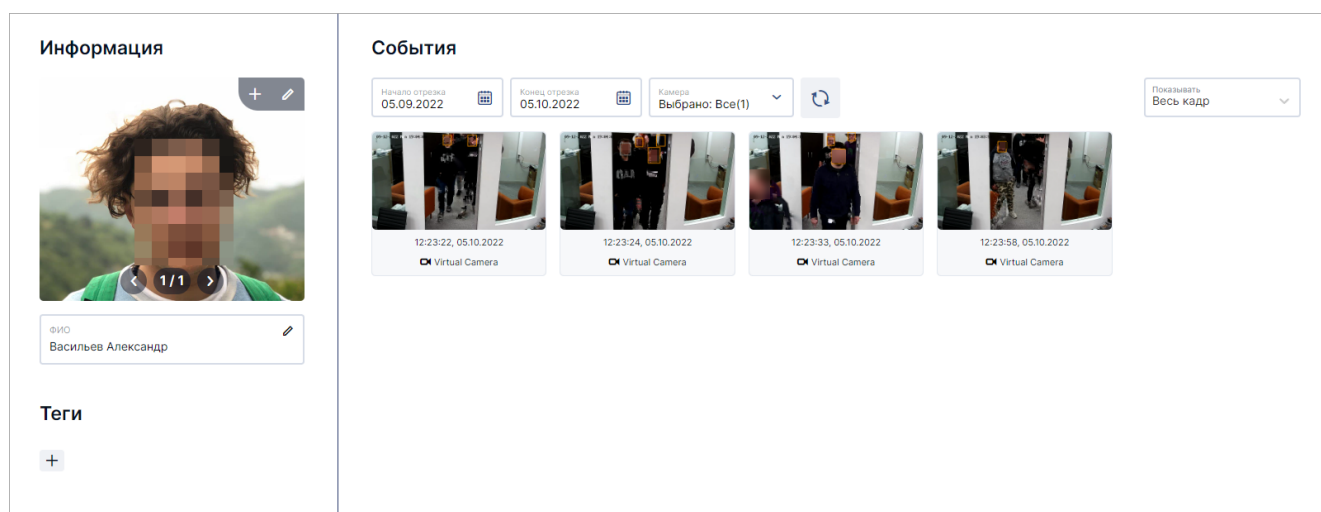


Для каждого человека отображается основное фото, ФИО, произвольное описание (если задано) и теги.

Поиск доступен по ФИО и содержимому полей с описанием.

События с персоной

Чтобы просмотреть, распознавал ли детектор человека, нажмите на строку с ФИО человека в списке персон.



В левой части экрана будет представлена информация о человеке, её можно редактировать.

Если на камере настроен **детектор идентификации лиц** и детектор распознал человека по фото, то в разделе События, будут показаны кадры, на которых детектор распознал этого человека.

В верхней части экрана возможно настроить отображение событий:

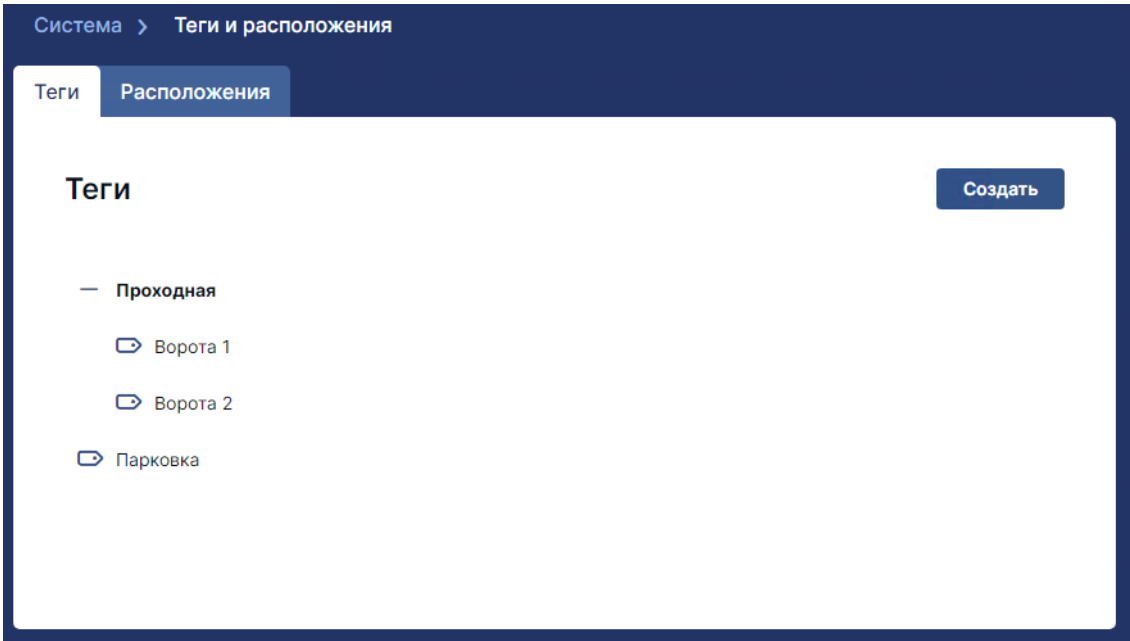
- **начало и конец отрезка** — показывать события только за определённый период времени;
- **Камеры** — выбрать, события с каких камер показывать;
- **Пreview** — отображать на превью в списке событий весь кадр или только лицо.

Справочник тегов и расположений

Теги используются для обозначения свойств и расположения камер.

Справочник тегов настраивается в разделе **Управление → Справочники → Теги и расположения камер**.

Теги можно присвоить камере на вкладке **Теги** в [настройках камеры](#).



Расположения — особые теги, предназначенные для обозначения расположения камеры. Расположению может быть присвоен краткий идентификатор, по которому камеры можно фильтровать при расширенном поиске.

Пользователи

Управление учётными записями пользователей осуществляется в разделе **Управление → Пользователи → Список пользователей**.

Пользователи						Добавить
Логин ↑	ФИО / Примечание	Доступ	Последний вход	Активные сессии	Журнал	
1user238	1	Разрешен	17.08.2026, 09:28:34			
2user238	2	Разрешен				
Admin	Admin	Разрешен	21.08.2026, 13:47:33	3		
1	1	Разрешен	21.08.2026, 12:36:46			

Первым представлен список пользователей системы.

Отображаются следующие данные о пользователях:

- логин;
- имя и примечание (если указано);
- статус доступа — разрешено ли пользователю входить в систему или нет. Определяется настройкой статуса аккаунта [в настройках учётной записи](#);
- время последнего входа;
- количество активных сессий при использовании Insentry под одним аккаунтом с разных браузеров или устройств.

Для перехода к [настройкам учётной записи](#), кликните по логину или имени пользователя в строке списка.

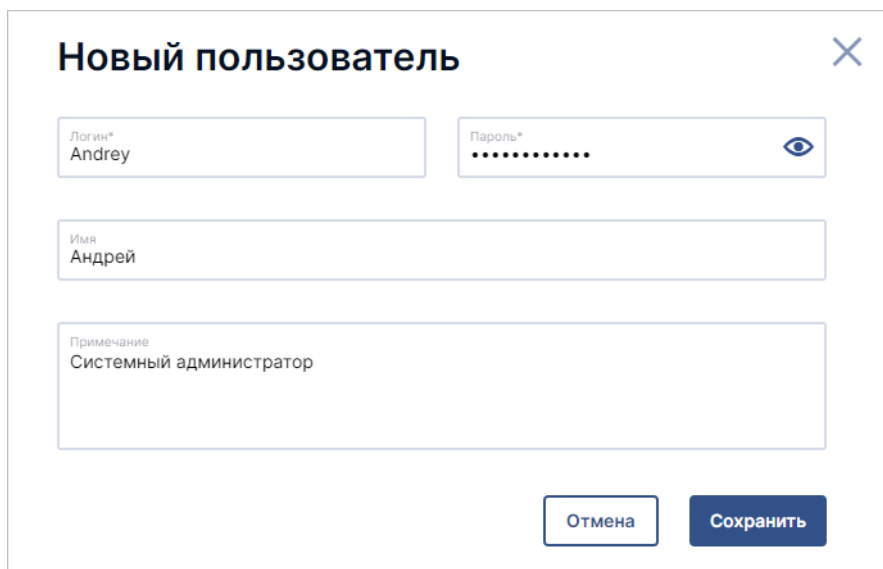
Для перехода к просмотру и экспорту [журнала операций](#) выбранного пользователя, воспользуйтесь кнопками в столбце **Журнал**.

Доступны следующие операции с учётными записями:

- [создание](#);
- [клонирование](#) — создание новой учётной записи на основе уже существующей, с такими же [правами доступа](#);
- [редактирование](#);
- [удаление](#);
- [просмотр лога действий](#).

Создание учётной записи

Чтобы создать новую учётную запись, перейдите в раздел **Управление → Пользователи → Список пользователей** и нажмите кнопку **Добавить пользователя**. Будет представлено окно создания новой учётной записи.



Новый пользователь ✕

Логин*
Andrey

Пароль*
..... 

Имя
Андрей

Примечание
Системный администратор

Отмена Сохранить

Укажите данные и подтвердите создание новой учётной записи.

Новый учётная запись будет отображена в списке пользователей.

[Настройте права доступа](#) нового пользователя к разделам системы — у новых пользователей нет никаких прав. При [дублировании существующей учётной записи](#) права доступа наследуются от пользователя, взятого за основу.

Логины пользователей должны быть уникальными.

Дублирование учётной записи

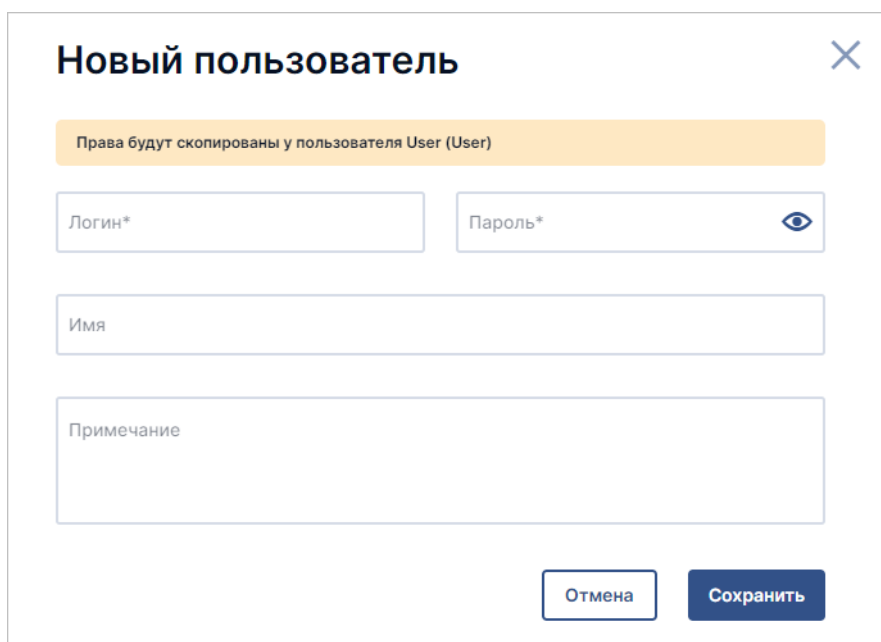
Чтобы создать учётную запись с такими же правами, как у существующего пользователя, удобно дублировать существующую учётную запись вместо того чтобы создавать новую.

При дублировании создаётся новая учётная запись с правами, аналогичными учётной записи, взятой за основу. У новой учётной записи определяются только имя, логин и пароль.

Чтобы дублировать учётную запись:

1. перейдите в раздел **Управление → Пользователи → Список пользователей**;
2. выделите строку в [списке пользователей](#);
3. нажмите кнопку  в конце строки.

Будет представлено окно параметров новой учётной записи:



Новый пользователь

Права будут скопированы у пользователя User (User)

Логин*

Пароль* 

Имя

Примечание

Отмена Сохранить

Все поля формы обязательные. Укажите данные и нажмите **Сохранить**.

Новый учётная запись будет отображена в [списке пользователей](#). Права новой учётной записи будут аналогичны правам исходной.

Настройки учётной записи

Чтобы настроить ранее созданную учётную запись:

1. Перейдите в раздел **Управление → Пользователи → Список пользователей**.
2. Выберите пользователя в [списке](#). Будет представлен раздел настроек учётной записи.
3. Откройте вкладку **Настройки**.

Для каждого пользователя возможно указать:

- **Статус** — активизация / деактивация учётной записи;
- **Логин** — логин пользователя;
- **Администратор** — права на настройку системы, камер, учётных записей других пользователей;
- **Изменить пароль** — пароль учётной записи;

- **Имя** — ФИО или должность сотрудника;
- **Примечание** — примечание свободного содержания.

The screenshot shows a web interface for managing users. At the top, there's a breadcrumb 'Пользователи > boss'. Below it, there are three tabs: 'Настройки' (Settings), 'Камеры' (Cameras), and 'Датчики' (Sensors). The 'Настройки' tab is active. It contains several fields and controls:

- Логин** (Login): A text input field containing 'boss'.
- Имя** (Name): A text input field containing 'Начальник охраны' (Security Chief).
- Изменить пароль** (Change password): A button.
- Администратор** (Administrator): A toggle switch, currently off.
- Пользователь активен** (User is active): A toggle switch, currently on.
- Примечание** (Note): A large text area.
- Может транслировать видео из приложения Insentry Mobile** (Can stream video from the Insentry Mobile app): A toggle switch, currently off.
- Сохранить изменения** (Save changes): A button at the bottom.

Смена пароля

Чтобы сменить пароль учётной записи:

1. Перейдите в раздел **Управление → Пользователи → Список пользователей**.
2. Кликните на имя пользователя в [списке](#). Будет представлен раздел настроек учётной записи.
3. Нажмите кнопку **Изменить пароль**.
4. Укажите новый пароль. Требования к паролю: только латинские буквы, не менее 6 символов, заглавная буква и цифра.
5. Сохраните изменения.

Назначение прав администратора

Администратор системы обладает правами на настройку системы, камер, учётных записей других пользователей.

Чтобы назначить пользователю права администратора:

1. Перейдите в раздел **Управление → Пользователи → Список пользователей**.
2. Кликните на имя пользователя в [списке пользователей](#). Будет представлен раздел настроек учётной записи.

3. Включите переключатель **Администратор**.
4. Сохраните изменения.

Трансляция из приложения

Если настройка **Может транслировать видео из приложения Insentry Mobile** включена, то пользователь может использовать приложение Insentry Mobile на смартфоне чтобы передавать видео с камеры мобильного устройства в Insentry Watch. Для этого пользователь должен быть авторизован в приложении, а также находиться в одной локальной сети с сервером Insentry.

Для начала трансляции нужно включить трансляцию в мобильном приложении Insentry Mobile.

Настройка прав доступа пользователя

Чтобы определить права доступа пользователя к управлению камерами, перейдите в раздел **Управление → Пользователи → Список пользователей** и кликните на имя пользователя в [списке пользователей](#). Будет представлен раздел настроек учётной записи. Перейдите на вкладку **Камеры**.

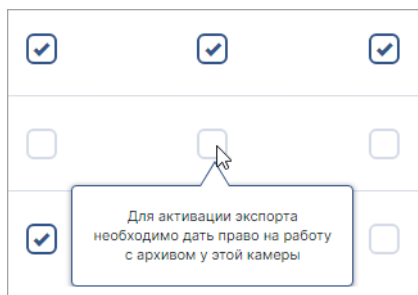
Чтобы разрешить пользователю управление определёнными настройками, установите отметку в соответствующем чек-боксе напротив нужной камеры.

Чек-боксы **наблюдение** и **Отчеты** предоставляют пользователю доступ к соответствующим разделам верхнего (главного) меню, если активированы хотя бы в одной камере. В [списке камер](#) отображаются все камеры, на которые у пользователя есть хоть какие-то права; в списке событий отображаются только события с камер, на которых пользователь имеет право смотреть архив.

Чек-бокс **PTZ** определяет поведение переключателя PTZ для выбранной камеры на странице просмотра видео в разделе **Просмотр** (см. *Руководство пользователя, раздел Просмотр живого видео и архива*).

Чек-бокс **Экспорт** определяет доступ к разделу **Экспорт** и поведение переключателя экспорта для выбранной камеры на странице просмотра видео в разделе **Архив**.

Права имеют вложенную структуру. Чтобы предоставить доступ к разделу PTZ (управление поворотными камерами), необходимо сперва предоставить доступ к наблюдению (просмотр потока камер), а чтобы разрешить экспорт архива, необходимо сперва разрешить работу с архивом. При наведении курсора мыши на права, требующие предварительного делегирования прав более высокого уровня, появляется всплывающая подсказка:



При клике на название камеры осуществляется переход в раздел [настройки камеры](#), где возможно на одном экране делегировать права доступа к управлению камерой для всех пользователей.

Список пользователей						
Логин	Наблюдение	Архив	Экспорт	Отчеты	PTZ	Настройки
Admin	☒	☒	☒	☒	☒	☒
2user238	☒	☒	☒	☒	☒	☒
1user238	☒	☒	☒	☒	☒	☒
1	☐	☐	☐	☐	☐	☐

При операции [дублирования учётных записей](#), права доступа для новой учётной записи наследуются идентично правам доступа учётной записи, взятой за основу.

Удаление учётной записи

Чтобы удалить учётную запись:

- перейдите в раздел **Управление → Пользователи → Список пользователей**;
- выделите строку в списке пользователей;
- нажмите кнопку удаления  в конце строки. Появится окно подтверждения операции.

При успешном удалении учётной записи в левой нижней части экрана будет представлено оповещение об этом.

Оповещение автоматически закрывается через указанное на таймере количество секунд.

Аудит действий пользователя

Все действия пользователей логируются в журнал.

В разделе **Управление → Пользователи → Аудит действий пользователя** показана информация о действиях пользователей в системе за последний месяц. Раздел доступен только администраторам.

Отслеживаются и сохраняются следующие действия:

- вход/выход пользователя;
- управление объектами системы:
 - выбор раскладок, вывод камер на раскладку;
 - управление PTZ-камерами;
 - вход/выход в режим просмотра архива, воспроизведение видео, экспорт записей и скриншотов;
 - экспорт событий и инцидентов;
 - создание/удаление контекстов;
 - подключение внешних систем, синхронизация конфигураций с внешними системами, отправка команд управления во внешние системы;
- изменение любых настроек в разделе **Управление**;
- добавление, изменение и удаление объектов в системе.

Просмотр списка операций

Аудит

Записей на страницу

Все

Экспорт

Время события ↑	Пользователь	Действие
14.07.2026, 17:36:43	Admin Admin	✓ Вход в систему Пользователь: Admin
14.07.2026, 17:34:13	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Запрос на открытие сессии просмотра live по камере Камера: test 20
14.07.2026, 17:33:12	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Завершение сессии просмотра live по камере Камера: test 27
14.07.2026, 17:29:12	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Запрос на открытие сессии просмотра live по камере Камера: test 27
14.07.2026, 17:28:13	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Завершение сессии просмотра live по камере Камера: test 32
14.07.2026, 17:24:12	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Запрос на открытие сессии просмотра live по камере Камера: test 32
14.07.2026, 17:23:13	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Завершение сессии просмотра live по камере Камера: test 26
14.07.2026, 17:19:12	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Запрос на открытие сессии просмотра live по камере Камера: test 26
14.07.2026, 17:18:13	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Завершение сессии просмотра live по камере Камера: test 27
14.07.2026, 17:14:12	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Запрос на открытие сессии просмотра live по камере Камера: test 27
14.07.2026, 17:13:13	D-rtMBZp6cRqGzNjdnmPFaD...	✓ Завершение сессии просмотра live по камере Камера: test 32
		✓ Запрос на открытие сессии просмотра live по камере

Тип пользователя

Пользователь

Ир-адрес клиента

127.0.0.1

Тип клиента

Веб-клиент

Дата и время

14.07.2026, 17:24:12

Объект действия

Камера

Тип действия

Запрос на открытие сессии просмотра live по камере

Результат действия

✓ Успешное

Слева показан список последних совершённых операций. Каждая запись содержит:

- логин пользователя;
- имя пользователя;
- роль пользователя;
- IP-адрес;
- тип действия;
- объект действия;
- параметры действия;
- точное (до секунд) время совершения операции;
- результат (успех/ошибка и текст ошибки, если есть);
- канал (веб-интерфейс, API, мобильное приложение).

Выберите запись в списке, чтобы увидеть подробности операции в правой части экрана.

В верхней части рабочей области вы можете настроить количество отображаемых записей на странице. Если записей больше, чем отображено, появляются кнопки пагинации.

Поиск и фильтрация списка операций

Поиск по ключевым словам осуществляется средствами браузера по нажатию Ctrl+F.

Для включения фильтрации нажмите кнопку фильтра справа от названия раздела в меню. Кнопка меняет вид в зависимости от состояния фильтра:

 — есть активный фильтр;

 — нет активных фильтров.

В верхней части рабочей области появится панель фильтрации. Фильтры настраиваются так же, как в других разделах системы.

Доступна фильтрация по следующим параметрам:

- типу действия;
- результату действия;
- пользователю;
- отрезку времени.

Внимание! Данные не обновляются автоматически. После настройки фильтров необходимо нажать кнопку «Обновить»  для применения изменений.

Для удаления отдельного фильтра нажмите на «крестик» рядом с настроенным фильтром. Для сброса всех фильтров нажмите большой «крестик» в правой части панели фильтрации.

Если настроено несколько фильтров, будут показаны записи, удовлетворяющие настройкам всех фильтров.

Экспорт списка операций

Чтобы выгрузить список операций и сохранить на локальный компьютер, нажмите кнопку **Экспорт**. Список сохраняется в виде json файла. Экспортируются записи, соответствующие условиям фильтра (если настроена фильтрация).

Пример записи:

```
{
  "timestamp": 1784039893226,
  "login": "user",
  "host": "192.168.13.239:59742",
  "objectType": "CAMERA",
  "objectId": "f5dc9ea5-2703-4065-a801-cfedj74b",
  "actionType": "LIVE_RELEASE",
  "actionParams": {
    "profile": "axxon0",
    "isAdmin": false
  },
  "actionSuccess": true,
  "clientType": "WEB"
},
```

Подключение Watch к каталогу LDAP (включение учетных записей Active Directory)

Если вы используете каталоги LDAP, вы можете подключить к ним Insentry, чтобы пользователи Active Directory могли авторизоваться на сервере видеонаблюдения без создания дополнительных учетных записей.

Пример подключения в домене insentry.local:

1. Остановите службу Insentry.Watch.Service в диспетчере задач.

InSentry.Cast.Service	4616	InSentry.Cast	Выполняется
InSentry.Keep.Service	4728	InSentry.Keep.Lite	Выполняется
InSentry.PTZ.Service	4684	InSentry.PTZ	Выполняется
InSentry.Spot.Metadata	4600	InSentry.Spot.Metadata	Выполняется
InSentry.Spot.Service	12032	InSentry.Spot.Lite	Выполняется
InSentry.Watch.Lite	4632	InSentry.Watch.Lite	Остановка

2. Перейдите в каталог InSentry.Watch, расположенный по адресу **C:\Program Files\InSentry\Watch.Lite**.

Этот компьютер > Локальный диск (C:) > Program Files > InSentry > Watch.Lite

Имя	Дата изменения	Тип	Размер
maps	01.05.2021 21:20	Папка с файлами	
plugins	01.05.2021 21:20	Папка с файлами	
application.properties	30.04.2021 10:11	Файл "PROPERTIES"	3 КБ
InSentry.WatchLite.exe	30.04.2021 10:11	Приложение	161 КБ
InSentry.WatchLite.ini	30.04.2021 10:11	Параметры конф...	1 КБ
install.bat	30.04.2021 10:11	Пакетный файл ...	1 КБ
monitoring.json	30.04.2021 10:11	Файл "JSON"	1 КБ
WatchLite.exe	30.04.2021 10:12	Приложение	87 310 КБ

3. Откройте файл `application.properties` с помощью любого текстового редактора.
4. Найдите строку `ldap.security.url=ldap` и уберите символ `#` в начале неё (раскомментируйте).
5. Вместо `ldap_addr` укажите IP адрес сервера LDAP, по умолчанию используется порт 389.
6. Вместо `dc=insentry,dc=local` укажите название используемого домена.

`\#ldap.security.url=ldap://ldap_addr:389/dc=insentry,dc=local`

7. Сохраните файл `application.properties`.
8. Запустите службу `InSentry.Watch.Service` через диспетчер задач.

После подключения при входе пользователя в систему, Watch будет проверять его логин не только по базе локальных пользователей, но и по каталогу LDAP.

Если в LDAP и локальной базе есть пользователи с одинаковым именем, то авторизоваться можно только с логином и паролем локальной учётной записи пользователя.

Подключения

В разделе **Управление → Подключения** вы можете настроить передачу данных в ЕЦХД и ГИС «Сфера», а также подключить бота для получения оповещений в приложении Telegram.

Настройка интеграции с ЕЦХД

Настройки, связанные с передачей данных в ЕЦХД, осуществляются в разделе **Управление → Подключения → ЕЦХД**.

Во вкладке **ЕЦХД** можно указать данные для авторизации в ЕЦХД с помощью basic или digest авторизации.

Во вкладке **Список камер** можно скачать список камер в формате, подходящем для ЕЦХД.

Используемый адрес сервера для доступа извне настраивается в разделе **Управление → Система → Адрес для внешних подключений** — см. [инструкцию](#).

1. Настройка модулей Cast и Keep

По требованию ДИТ нужно передавать видеопотоки через 554 порт и настроить работу HTTP-сервера с API ЕЦХД работает через 80 порт. Чтобы выполнить эти требования:

1. В файле конфигурации модуля Cast в строке параметра **rtsp.port** укажите значение **554** вместо **5540**.

Расположение файла конфигурации модуля Cast: - Linux:

/usr/src/InSentry/Cast/application.properties - Windows: C:\Program

Files\InSentry\Cast\application.properties (пусть при установке по умолчанию)

2. В файле конфигурации модуля Keep в строке параметра **server.port** укажите значение **80**.

Расположение файла конфигурации модуля Keep: - Linux:

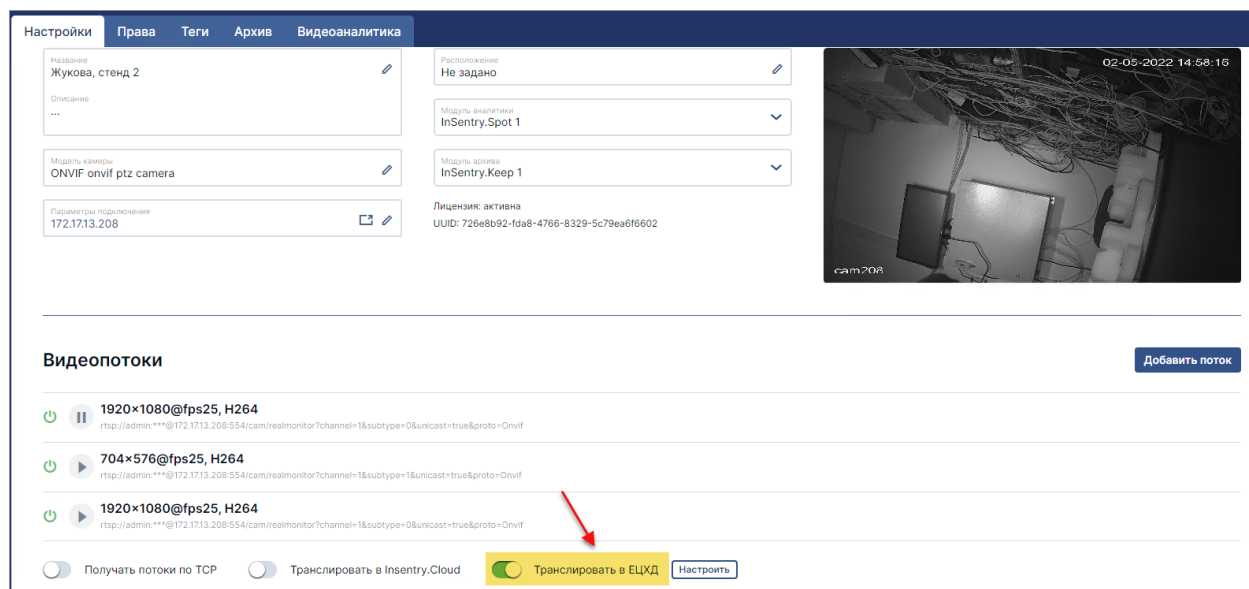
/usr/src/InSentry/Keep/application.properties - Windows: C:\Program

Files\InSentry\Keep.Lite\application.properties (пусть при установке по умолчанию)

3. Перезапустите службы Cast и Keep.

2. Включение передачи данных в ЕЦХД в настройках камеры

1. Перейдите в раздел **Управление → Устройства → Камеры** → клик по строке с описанием камеры (**Настройки камеры**) → вкладка **Настройки**.
2. Включите трансляцию в ЕЦХД:



3. Формирование списка адресов

Через API, описанное в [официальном регламенте](#), данные в ЕЦХД автоматически не поступают. Необходимо передать в ДИТ внешний адрес сервера, а также списки URL сервера и адресов для получения видеопотоков и архивов.

1. Перейдите в раздел **Управление → Система → Адрес для внешних подключений**.
2. Выберите из списка или укажите IP, по которому ЕЦХД сможет получить доступ к данным камер. Поле **Переопределение порта** оставьте пустым, иначе потоки камер не будут воспроизводиться по внешним ссылкам. Нажмите кнопку **Сохранить**.
3. Перейдите в раздел **Управление → Импорт/экспорт → Экспорт списка камер в формате ЕЦХД** и скачайте список камер для передачи в ДИТ.

Файл будет загружен на локальный компьютер. Место расположения файла определяется настройками браузера. Чтобы просмотреть список загруженных файлов в Google Chrome, нажмите Ctrl+J / Command+J.

4. Настройки авторизации в ЕЦХД

В разделе **Управление → Система → Настройки ЕЦХД** можно указать данные для авторизации в ЕЦХД с помощью basic или digest авторизации.

5. Проверка работоспособности интеграции с ЕЦХД

Для проверки работоспособности интеграции с ЕЦХД:

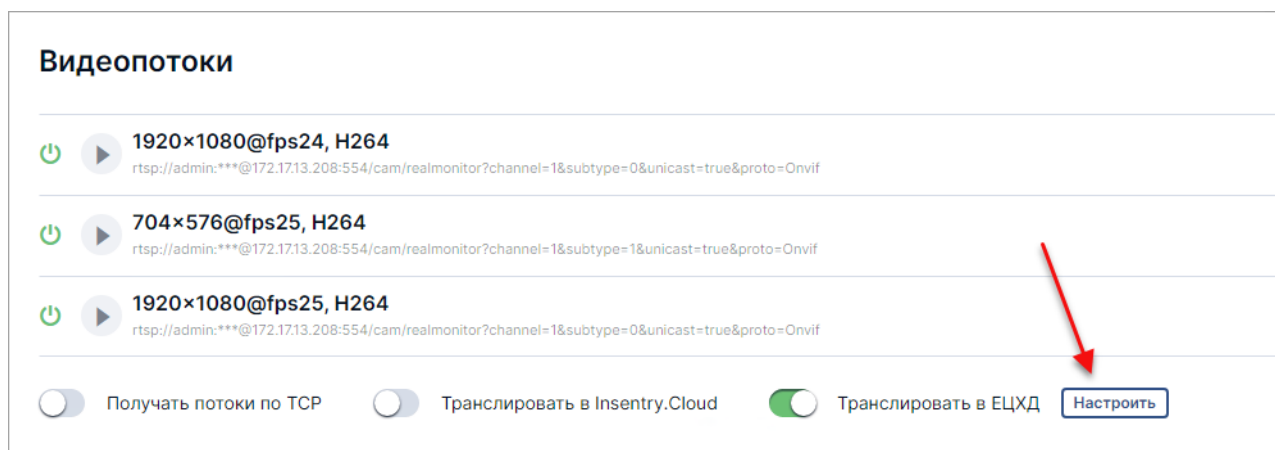
1. Ознакомьтесь с [регламентом интеграции с ЕЦХД](#) (Приложение 3, раздел 9).
2. Проверьте API для получения списка камер (см. регламент):
`http://device-address/getcameras`, где `device-address` это адрес сервера.
3. Проверьте API для получения видеопотока (см. регламент):
`http://device-address/getliveurl?cameraid=1`, где `device-address` это адрес сервера.

4. Проверьте API для получения архивов потоков (см. регламент):
`http://device-address/getarchiveurl?cameraid=1`, где `device-address` это адрес сервера.
5. Проверьте [доступность потока при помощи VLC-плеера](#). Используйте тот URL, к которому будет обращаться система ЕЦХД.
6. Проверьте доступность архивного видео при помощи VLC-плеера. Используйте тот URL, к которому будет обращаться система ЕЦХД. Архив должен начать проигрываться с самого первого интервала.

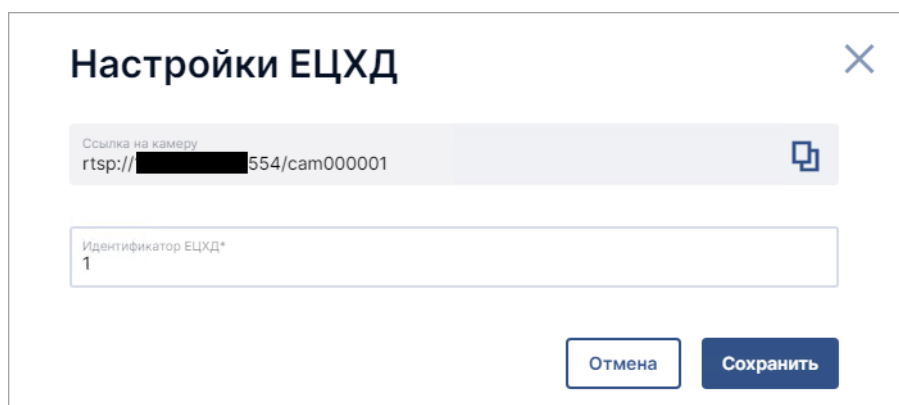
Как посмотреть URL камеры и адрес потока

Перейдите в раздел **Управление → Устройства → Камеры → Настройки камеры** (вкладка **Настройки**). В нижней части экрана представлен блок [управления видеопотоками](#).

Нажмите кнопку **Настроить** рядом с переключателем **Транслировать в ЕЦХД**.

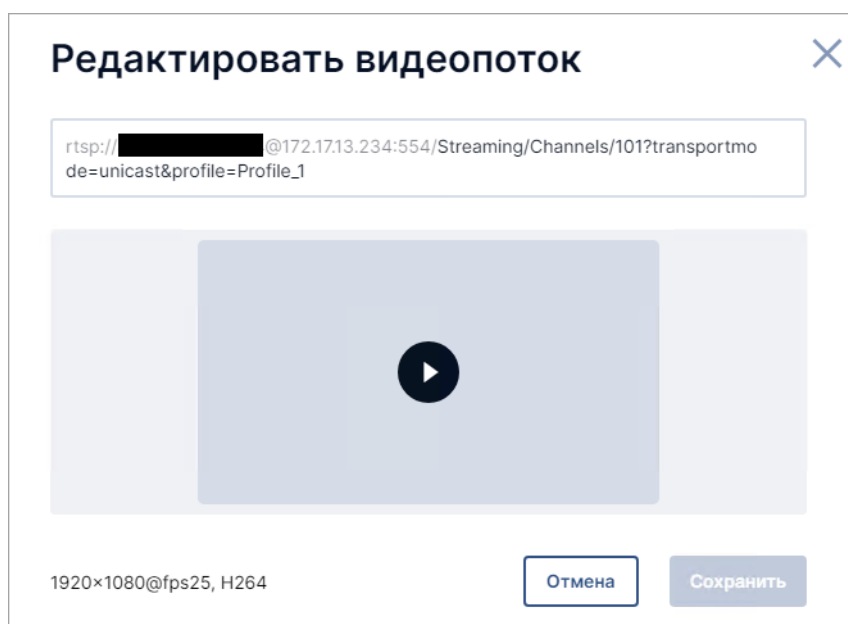


Ссылка на URL камеры расположена в верхнем поле. Чтобы скопировать её в буфер обмена, нажмите кнопку .



Как посмотреть адрес потока

Перейдите в раздел **Управление → Устройства → Камеры → Настройки камеры** (вкладка **Настройки**). В нижней части экрана представлен блок [управления видеопотоками](#).



Перейдите к редактированию потока и скопируйте полный адрес потока с логином и паролем.

Как посмотреть адрес сервера

Используемый адрес сервера для доступа извне настраивается в разделе **Управление → Система → Адрес для внешних подключений**.

Нормативные документы и контакты ЕЦХД Москвы

[Нормативные документы ЕЦХД](#)

[Контакты ЕЦХД](#)

Настройка интеграции с Telegram ботом

Бот в Telegram оповещает о событиях с детекторов, статусе работы камер и видеоаналитики, присылает скриншоты с камер.

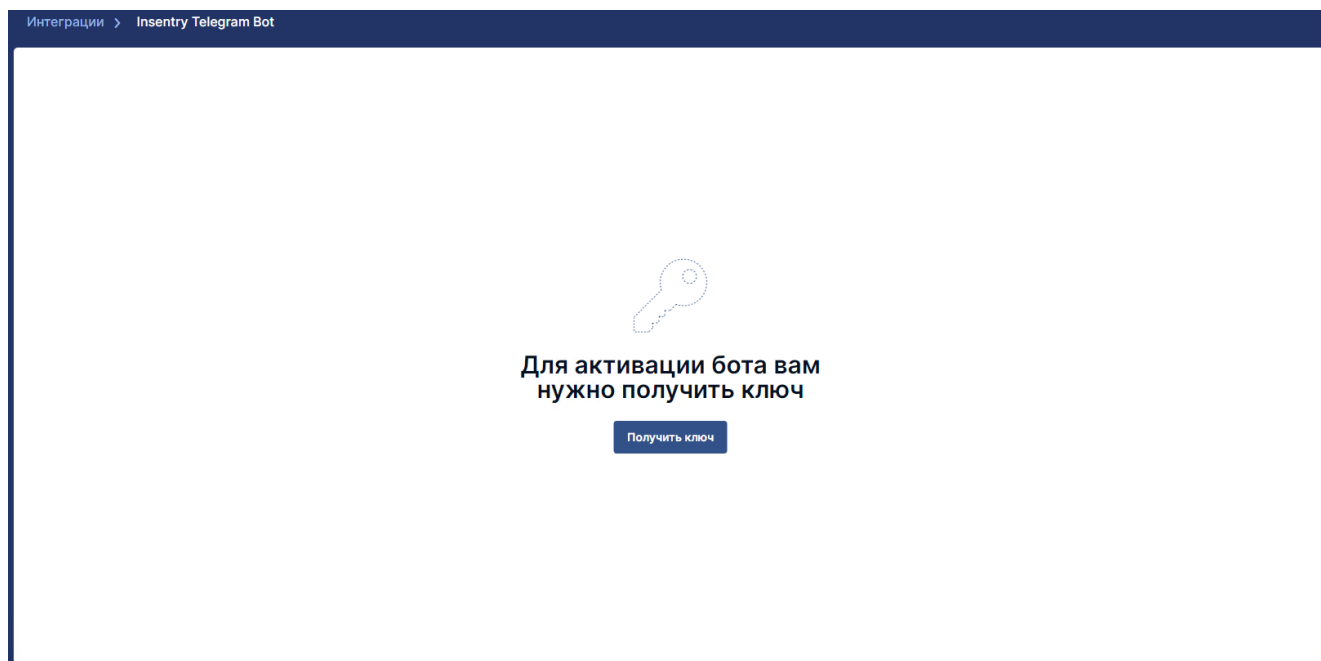
Бот настраивается администратором в разделе **Управление — Интеграции — Insentry Telegram Bot**. После настройки интеграции любой пользователь может добавить бот в свою учётную запись Telegram с помощью ссылки или QR-кода в личном кабинете.

Чтобы бот работал, сервер, где установлено ПО Insentry, должен иметь доступ в интернет.

Получение ключа

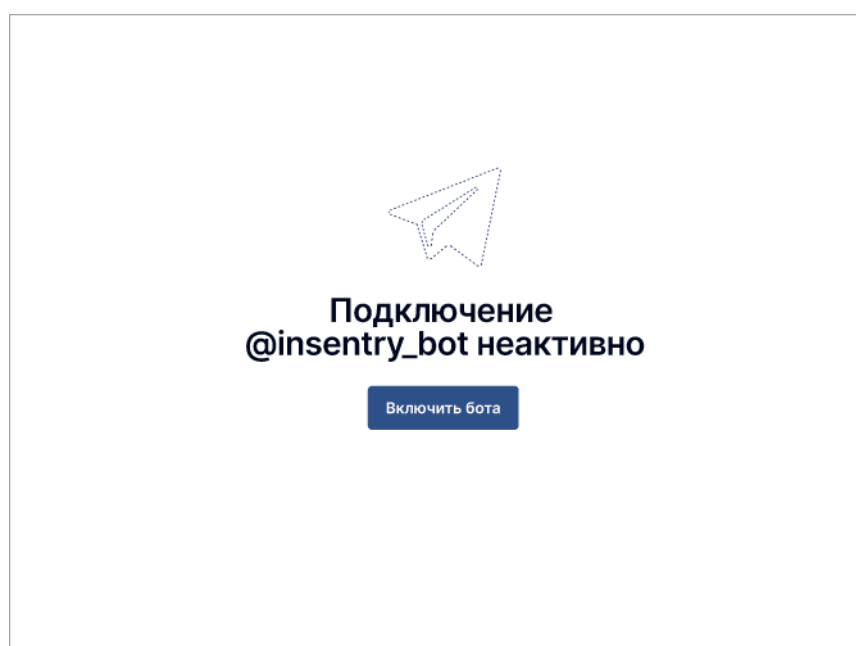
Этот шаг нужен только пользователям бесплатной лицензии. Если вы используете платную лицензию, то она уже активирована, и вам нужно только подключить бот.

Нажмите **Получить ключ** и заполните анкету на сайте <https://insentry.io/ru/get-license-key>, чтобы получить бесплатный ключ лицензии. Ключ придёт вам на почту. Активируйте его [по инструкции](#).

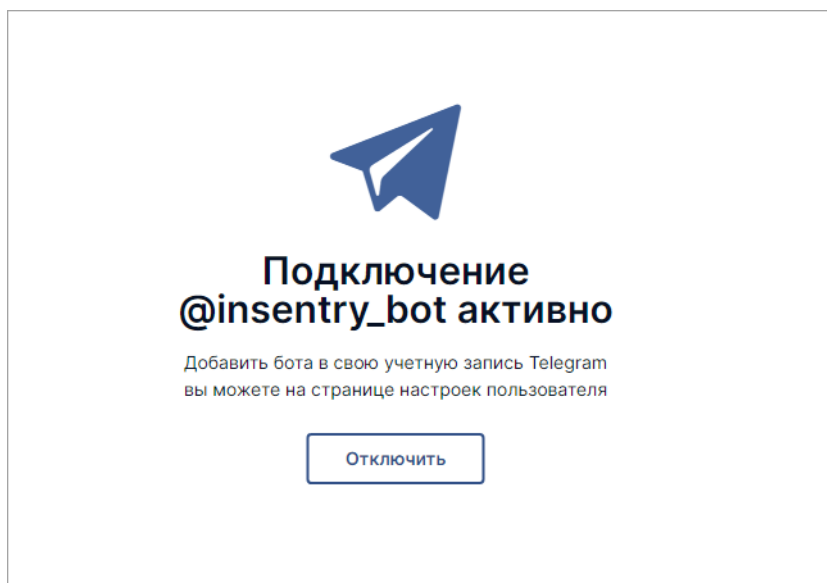


Настройка интеграции

Интеграцию настраивает администратор в разделе **Управление — Интеграции — Insentry Telegram Bot**.



Чтобы включить интеграцию, нажмите кнопку **Включить бота**.

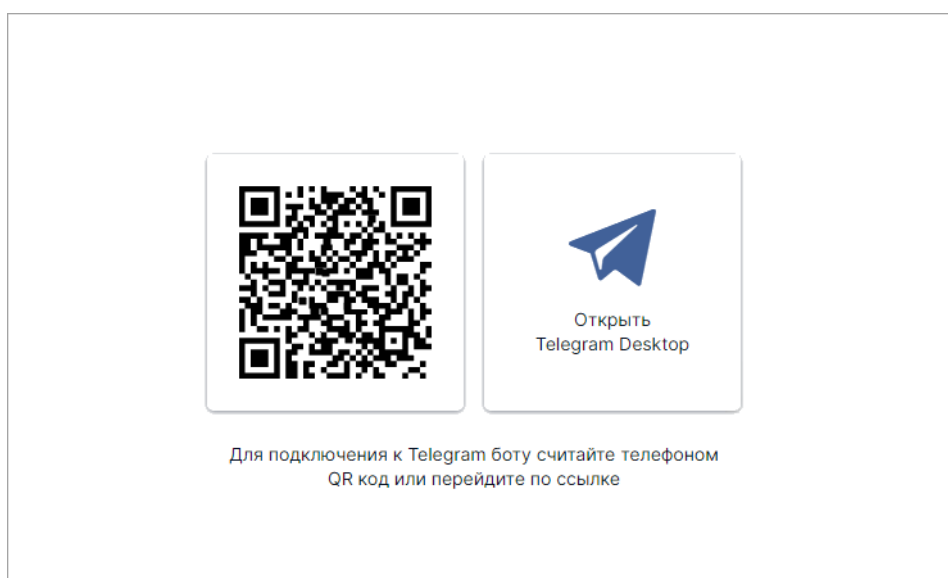


Подключение бота

Чтобы начать использовать бот, добавьте его в свою учётную запись Telegram в разделе **Личный кабинет — Telegram бот**.

Для этого считайте телефоном QR-код на экране или перейдите по ссылке, которая откроет бот в приложении Telegram.

QR-код позволяет связать аккаунт пользователя Insentry только с одним аккаунтом Telegram. Чтобы добавить бот нескольким пользователям Telegram, подключите бот с помощью QR-кодов отдельно в каждой учётной записи Insentry. Интеграцию повторять не нужно — достаточно настроить её один раз, чтобы она работала во всех учётных записях Insentry.



ГИС «Сфера»

Интеграция позволяет передавать лица, распознанные детектором, в ГИС «Сфера».

Данные для интеграции необходимо получить в ГИС «Сфера» и указать в разделе **Управление → Система → Интеграции → ГИС «Сфера»**.

ГИС «Сфера»

☒ Передача данных в «Сферу»

Чтобы включить передачу данных, обязательно укажите и сохраните URL, логин и пароль в настройках справа.

передача данных	15.05.2025, 15:25:28
Последняя неуспешная передача данных	15.05.2025, 15:25:28
Статус подключения	Норма
Успешно передано	59245
Ошибки при передаче	2

Настройки

URL

https://

Логин*

Root

Пароль*

👁

Сохранить

Настройки системы

Диагностика на основе лог-файлов

В разделе **Управление → Система → Диагностика** вы можете просмотреть журналы логов работы модулей системы.

Доступны три вида журналов:

- логи модулей системы;
- логи модуля Watch;
- логи действий пользователей.

Логи выводятся списком. Самые ранние записи отображаются внизу списка. Журнал автоматически пополняется новыми записями. Для быстрого возврата к самым свежим записям нажмите кнопку **Показать последние логи**.

Настроенные фильтры и контекст (см. *Руководство пользователя, раздел Контекст и фильтрация данных*) к журналам логов не применяются.

С помощью выпадающего списка в правом нижнем углу вы можете отфильтровать логи по уровню важности:

- **DEBUG** – отладочные сообщения для разработчиков;
- **INFO** – общая информация о работе приложения (старт, конфигурация, ключевые бизнес-события);
- **WARNING** – предупреждения о потенциальных проблемах (например, deprecated API, нехватка ресурсов);
- **ERROR** – ошибки, которые нарушают работу функции, но не останавливают приложение.

Чтобы скачать журнал логов в виде *.txt файла, нажмите кнопку **Скачать** и сохраните файл на локальный компьютер.

Система серверов

Система серверов объединяет несколько серверов Insentry в единую иерархическую инфраструктуру, позволяющую пользователям соседних узлов просматривать потоки камер, архив, события и инциденты с других узлов, входящих в единую систему.

Отказоустойчивость каждого узла обеспечивается развёртыванием Insentry в кластерной конфигурации Active/Passive или Active/Active. Администрирование, управление и мониторинг кластера выполняются за пределами Insentry.

Иерархия серверов в системе

Топология системы серверов представляет собой дерево. Корневой сервер в системе может быть только один. Каждый узел может входить в состав только одной системы серверов.

Иерархия родитель-потомок определяет топологию системы и положение каждого узла в ней. Каждый узел имеет не более одного узла-родителя и произвольное число узлов-потомков. Узел, не имеющий узла-родителя, является корневым узлом системы.

Отношения доверия

Отношения доверия предоставляют узлам доступ к объектам других узлов.

Доверие узла А узлу В предоставляет узлу В доступ к следующим объектам и данным узла А:

- просмотру состояния подключенных камер и устройств в интегрированных внешних системах;
- просмотру статуса подключения внешних систем;
- просмотру событий, полученных от устройств и детекторов на узле А, и инцидентов, сформированных по таким событиям;
- живому видео и архиву камер, подключенных к узлу А.

Данное отношение задаётся между соседними серверами: родителем и потомком. Отношение доверия может быть однонаправленным или двунаправленным.

Поддерживаются два типа отношений доверия между узлами:

- нетранзитивное (базовое) доверие — если узел А доверяет узлу В нетранзитивно, то узел А предоставляет доступ узлу В только к собственным объектам и данным. Объекты и данные, к которым А имеет доступ через собственные отношения доверия с другими узлами, узлу В недоступны.
- транзитивное доверие — если узел А доверяет узлу В транзитивно, то узел А предоставляет узлу В доступ к своим данным не только серверу В, но и серверам-родителям узла В, которым узел В доверяет. Таким образом, доверие наследуется вверх по иерархии.

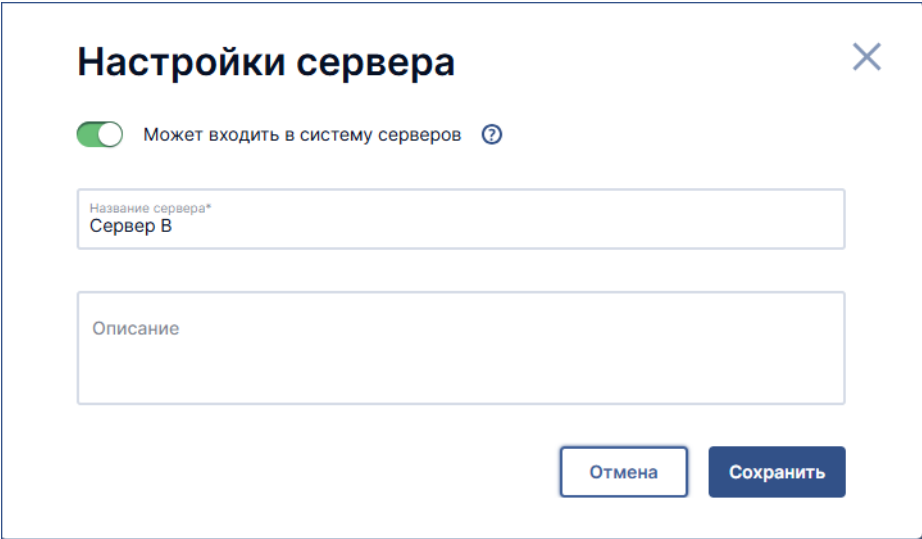
Транзитивность может быть настроена для каждого направления доверия по отдельности.

Права доступа конкретных пользователей определяются правами их учётных записей.

Режимы работы сервера

Сервер функционирует в одном из двух режимов: автономно либо в составе распределённой системы.

По умолчанию сервер работает в автономном режиме и не может входить в состав распределённой системы. Перевод сервера в режим работы в составе распределённой системы выполняется через диалоговое окно настройки параметров сервера в разделе **Управление → Система → Система серверов**.



Настройки сервера

☒ Может входить в систему серверов ?

Название сервера*
Сервер В

Описание

Отмена Сохранить

Для добавления сервера в систему необходимо указать имя сервера. Имена всех серверов, объединённых в систему, должны быть уникальными в рамках системы.

Сразу после активации переключателя **Может входить в систему серверов** сервер переходит в режим работы в составе распределённой системы, однако ещё не является участником ни одной такой системы. Для формирования распределённой системы администратор сервера принимает входящий запрос на добавление либо инициирует добавление самостоятельно.

Если сервер входит в состав распределённой системы, деактивация переключателя удаляет его из системы. При этом будут разорваны его связи с узлами-родителем и узлами-потомками.

Добавление сервера в систему

Сервер, переведённый в режим работы в составе системы серверов и имеющий заданное имя, может принимать входящие запросы на включение в существующую распределённую систему в качестве узла-потомка сервера, с которого поступил запрос.

Шаг 1. Установление связи с сервером

Для добавления сервера в систему серверов, на локальном сервере в разделе **Управление → Система → Система серверов** нажмите кнопку **Добавить**. Откроется диалоговое окно добавления сервера.

Исходящий запрос формируется от узла-родителя в адрес узла-потомка.

Введите IP-адрес и порт добавляемого сервера (по умолчанию — 9200).

Шаг 2. Параметры доверия

Укажите желаемые параметры отношения доверия для добавляемого узла-потомка и нажмите кнопку **Отправить**.

Система попытается подключиться к нему и автоматически проверит, что:

- сервер не работает в автономном режиме;
- сервер не состоит в другой системе серверов.

Если хотя бы одна проверка не пройдена, система выводит сообщение об ошибке, и процедура прерывается.

Шаг 3. Отправка запроса

На добавляемый сервер отправляется запрос.

Принять или отклонить запрос может только администратор сервера. В интерфейсе отображается только последний поступивший запрос. Запрос действителен в течение 5 минут с момента поступления. Если администратор сервера не принял запрос в течение указанного времени, отправителю направляется уведомление об истечении времени ожидания, а запрос удаляется.

Запрос на добавление содержит параметры отношения доверия, с которыми данный сервер будет включён в систему. При принятии запроса администратор сервера вправе изменить параметры доверия со своей стороны. Изменение параметров доверия также доступно после добавления сервера в систему.

Запрос на добавление узла-потомка

IP адрес узла-потомка
127.0.0.1

Порт HTTP
12345

☒ Доверять узлу

☒ Доверять узлу транзитивно

☒ Запросить доверие текущему узлу

☒ Запросить транзитивное доверие текущему узлу

Отмена

Отправить

Шаг 4. Обработка запроса

На сервере-родителе во вкладке **Исходящие запросы** отображается список серверов, которым был отправлен запрос и от которых ещё не получен ответ.

Система серверов

Исходящие запросы

Входящие запросы

Исходящие запросы

IP адрес или hostname	Название / Описание	Доверие ?	Статус запроса	Дата запроса	Время жизни
172.17.17.17:9230		△	Не доставлен	06.08.2026, 12:17	
172.17.17.17:9230	239	△	Принят	06.08.2026, 12:11	
172.17.17.17:9230	Сервер BB	▲	Принят	06.08.2026, 12:07	

Процедура добавления завершается только после того, как администратор добавляемого сервера примет запрос.

При обработке входящего запроса на сервере-потомке администратор сервера может изменить параметры доверия серверу-родителю, от которого пришёл запрос.

Система серверов

Исходящие запросы

Входящие запросы (1)

Входящие запросы

Название родителя

Название сервера

IP адрес

192.0.0.1:5000

Описание

Описание сервера

Дата отправки запроса

15.05.2025, 15:30

Время жизни запроса

0:34

Доверять узлу-родителю

Доверять узлу-родителю транзитивно

Узел-родитель доверяет текущему узлу

Узел-родитель доверяет текущему узлу транзитивно

Отклонить

Принять

При принятии запроса система выполняет проверку уникальности имени сервера в пределах системы серверов.

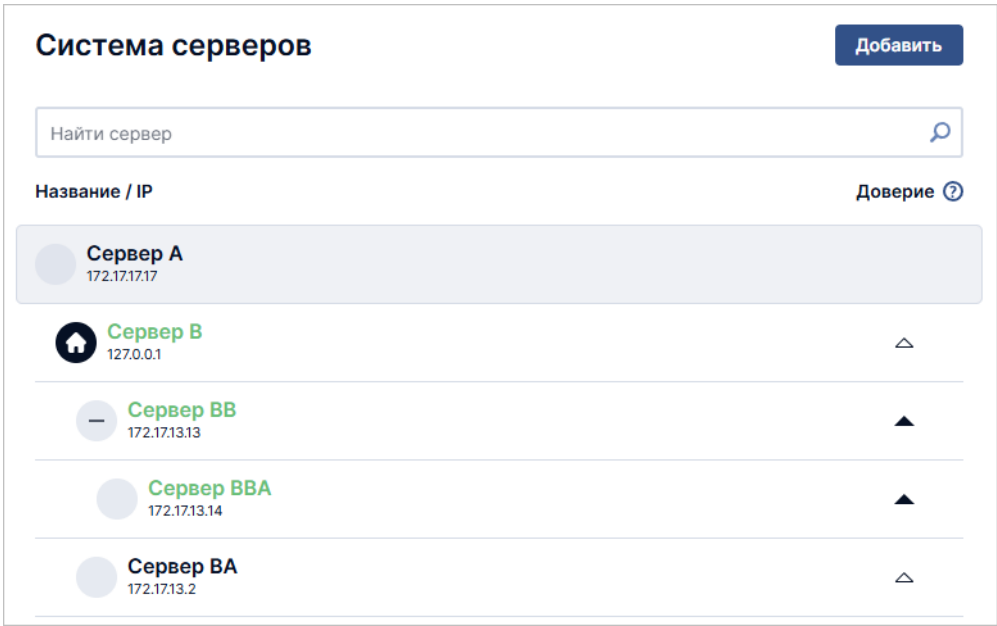
Если администратор принял запрос — сервер добавляется в систему серверов. Если администратор отклонил запрос — запрос останется в списке, но сервер не будет добавлен в систему.

Просмотр списка серверов, входящих в систему

Как только администратор текущего сервера переводит сервер в режим распределённой работы, в разделе **Управление → Система → Система серверов** показан список серверов, входящих в систему.

В поле поиска можно вводить целиком или частично название или IP-адрес серверов для быстрого поиска. При нахождении совпадений автоматически раскрываются все вышестоящие узлы дерева, чтобы найденный сервер был виден в контексте иерархии.

При выборе сервера в списке зелёным цветом подсвечиваются все серверы, имеющие отношения доверия с выбранным узлом.



Обозначение	Описание
	Текущий сервер
	Узел, имеющий дочерние серверы. Нажмите, чтобы раскрыть
	Недоступный узел

Изменение параметров параметры отношения доверия

Изменить параметры отношения доверия на сервере может только его локальный администратор.

Для этого:

1. Перейдите в раздел **Управление → Система серверов**.
2. Выберите нужный сервер в списке и откройте его настройки, кликнув по строке с именем нужного сервера-родителя или потомка текущего сервера.
3. Нажмите кнопку **Подробнее** в правой части экрана.
4. Перейдите на вкладку **Настройки**.
5. Задайте параметры доверия в отношении выбранного сервера.
6. Сохраните изменения.

Изменение отношений родитель-потомок

Для изменения отношения родитель-потомок:

1. Удалите нужный сервер из системы.
2. Заново добавьте его в систему в качестве потомка нужного узла.

Удаление сервера из системы серверов

Сервер можно удалить из системы двумя способами:

- администратор локального сервера отключает переключатель режима работы в разделе **Управление → Система → Система серверов**;
- администратор вышестоящего узла выполняет команду удаления для выбранного сервера в дереве системы серверов.

Если у удаляемого сервера есть узлы-потомки, из системы удаляется вся ветка целиком.

Серверы этой ветки остаются связанными между собой отношениями доверия, но отделяются в другую систему серверов, не связанную с предыдущей.

Если удаляется корневой сервер, то поведение системы определяется настроенной топологией:

- если у корневого узла есть только один узел-потомок, то он становится корневым сервером текущей системы серверов;
- если у корневого узла есть несколько узлов-потомков, то каждый из них становится корневым узлом для отдельных систем серверов, не связанных между собой.

При удалении сервера из системы прерываются все его отношения доверия с узлом-родителем и потомками, а также транзитивные отношения доверия, которые проходили через него.

Модули

Модули Insentry:

1. **Watch** — сервер системы видеонаблюдения, обеспечивающий основные функции системы;
2. **Cast** — подсистема для ретрансляции видеопотоков;
3. **Keep** — подсистема архивации, где сохраняются и воспроизводятся аудио- и видеопотоки, полученные от камер;
4. **Spot** — подсистема видеоаналитики, которая обеспечивает работу детекторов и анализ сцены;
5. **Common** — общие компоненты системы;
6. **Message Broker** — передача сообщений между компонентами системы;
7. **Get** — получение событий и сигналов от внешних систем;
8. **Mediator** — сохранение событий видеоаналитики;
9. **Metadata** — хранение метаданных.

Модули разворачиваются на сервере и обеспечивают функционирование клиентов системы видеонаблюдения в браузере на рабочих местах пользователей.

Модули Watch, Common и Cast должны быть установлены обязательно — без них система не будет работать, остальные модули можно не устанавливать, если они не нужны.

Список модулей представлен в разделе **Управление → Система → Модули**.

Модули								
Название	Версия	Тип	Статус	Режим	IP-адрес	Камеры	Описание	Журнал
 Cast 1 26.1.31.9			 Включен	Активен	127.0.0.1	35	Видеошлюз	 
 GET 1 26.1.31.24			 Включен	Активен	127.0.0.1	35	Внешние события	 
 Keep 1 26.1.31.7			 Включен	Активен	127.0.0.1	34	Видеоархив	 
 Mediator 1 26.1.31.7			 Включен	Активен	127.0.0.1	35	Служба сохранения событий	 
 MessageBroker 1 26.1.31.15			 Включен	Активен	127.0.0.1	35	Брокер сообщений	 
 Spot 1 26.1.31.8			 Включен	Активен	127.0.0.1	34	Видеоаналитика	 

Просмотреть и скачать логи можно в разделе **Управление → Система → Диагностика**, либо нажав на кнопку просмотра или сохранения в столбце **Журнал**.

Настройка модуля Кеер и параметров хранения архива

Модуль Кеер обеспечивает хранение видеоархива.

Архив сохраняется в хранилище на локальном жестком диске или сетевой папке. Хранилище может содержать один или несколько каталогов. После установки системы автоматически выделяется 10 Гигабайт для хранения архива в каталоге программы. По умолчанию — `C:\ProgramData\InSentry\Keep.Lite\video\folder`.

Настройки модуля: **Настройки → Модули → Кеер**.

Во вкладке **Настройки** отображена текущая структура хранилища.

Параметры хранилища:

- **Диск** — имя диска, на котором расположено хранилище;
- **Объём диска** — объём хранилища;
- **Свободно на диске** — остаток свободного места на диске, не занятого хранилищем;
- **Каталог** — путь к каталогу, куда записываются данные;
- **Лимит** — максимальный объём записанных данных в этом каталоге;
- **Занято архивом** — объём места на диске, занятый уже записанным архивом.

Во вкладке **Камеры** показан список камер, на которых [настроена запись в архив](#).

Модули > InSentry.Keep 1 Видеоархив						
Хранилища Камеры Настройки						
Хранилища						
Local storage						
Диск	Режим записи	Объем диска	Свободно на диске	Каталог	Лимит	Занято архивом
C:\	Включена	237 ГБ	78 ГБ	C:\ProgramData\InSentry\Keep.Lite	30 ГБ	3 ГБ
Итого		237 ГБ	78 ГБ		30 ГБ	3 ГБ
Добавить каталог						

Добавление каталога

Чтобы добавить каталог в хранилище:

1. Перейдите в настройки хранилища: **Управление → Модули → Кеер**.
2. Нажмите кнопку **Добавить каталог**.

Новый каталог

Диск

D:\ доступно 32 Гб из 930 Гб

D:\ доступно 32 Гб из 930 Гб

Новый сетевой каталог

Новый S3

Лимит, Гб*

☐ Только чтение ?

Отмена

Добавить

Параметры нового каталога:

- **Диск** — расположение на локальном жёстком диске, в сетевой папке или в облаке;
- **Лимит** — объём, выделяемый для хранилища, в гигабайтах. Значение должно быть больше нуля и не превышать доступного объёма выбранного диска;
- **Папка** — папка на выбранном диске или сетевой папке. Формат — путь к папке без указания корневого расположения. К примеру, если расположение папки C:\VideoArchive\folder, то в данном поле следует указать значение VideoArchive\folder.

Переключатель **Только чтение** позволяет добавить каталог, доступный только для чтения.

Новые файлы архива в эту папку записываться не будут, но уже записанный архив из неё будет доступен.

Для настройки записи архива в облако:

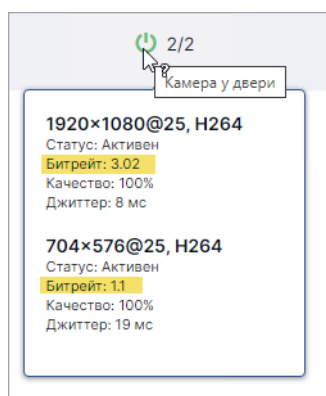
- проверьте, что модуль Metadata установлен и соответствующая служба запущена;
- в файле application.properties модуля Keep установите значение metadata.enabled=true;
- перезапустите службу InSentry.Keep;
- в настройках нового каталога выберите в поле **Диск** значение **Новый S3**;
- установите лимит, не превышающий объёма облачного хранилища, в противном случае запись будет остановлена;
- укажите путь к папке в облаке, логин и пароль.

Подключение к облачному каталогу может занять несколько минут.

Таким способом можно добавить только общедоступную сетевую папку, для доступа к которой не нужен логин и пароль. Чтобы добавить каталог, доступ к которому ограничен, нужно [разрешить учётной записи System использовать хранилище](#).

Расчёт лимита

Планируйте объём каталога для хранилища исходя из того, сколько потоков, какого качества и с какой глубиной вам нужно [записывать в архив](#). Для этого умножьте значения количества камер, их битрейт и глубину архива. Битрейт потока в мбит/с указан при наведении курсора на статус потока в [списке камер](#).



Если вам нужно рассчитать объём архива с нескольких камер и битрейт их потоков сильно различается, используйте для расчёта поток с наибольшим битрейтом, чтобы создать архив с запасом места.

Например: нужно рассчитать объём хранилища для 20 потоков с различным битрейтом, самый высокий — 0,4 мбит/с, глубина хранения — 30 суток.

1. Переводим битрейт из мбит/с в Гбит/с: $0,4 \div 1024 = 0,00039$ Гб/с.
2. Рассчитываем значение за 30 суток: $0,00039 \times 60 \times 60 \times 24 \times 30 = 1\,025,94$ Гб за 30 суток.
3. Умножаем на количество потоков, получаем 20 518,9 Гбит за 30 суток записи 20 потоков.
4. Переводим в гигабайты и округляем: $20\,518,9 \div 8 = 2564,9$ Гбайт или 2,6 Терабайт.

Итого: потребуется хранилище объёмом 2,6 Терабайт (с запасом, так как расчёт произведён для потока с наивысшим битрейтом).

Запись архива одного потока камеры FullHD H264 с глубиной 30 дней занимает примерно 1,5 ТБ.

Размер хранилища в любом случае не будет превышен, однако, если его недостаточно для записи всех выбранных потоков с указанной глубиной, то глубина записи может быть автоматически уменьшена, не дожидаясь переполнения.

Редактирование каталога

Чтобы редактировать каталог, нажмите на кнопку редактирования  в конце строки.

Откроются настройки каталога.

Настройки каталога

Диск: C:\

Лимит, ГБ*: 30

Папка: C:\ProgramData\InSentry\Keep.Lite

☐ Только чтение ?

Отмена Сохранить

Параметры каталога:

- **Диск** — расположение на локальном жёстком диске или в сетевой папке;
- **Лимит** — объём, выделяемый для хранилища, в гигабайтах. Значение должно быть больше нуля и не превышать доступного объёма выбранного диска;
- **Папка** — папка на выбранном диске или сетевой папке. Формат — путь к папке без указания корневого расположения. К примеру, если расположение папки C:\VideoArchive\folder, то в данном поле следует указать значение VideoArchive\folder.

Переключатель **Только чтение** позволяет добавить каталог, доступный только для чтения. Новые файлы архива в эту папку записываться не будут.

Редактирование названия хранилища

Чтобы изменить название хранилища, нажмите кнопку редактирования  напротив названия хранилища:

Хранилища

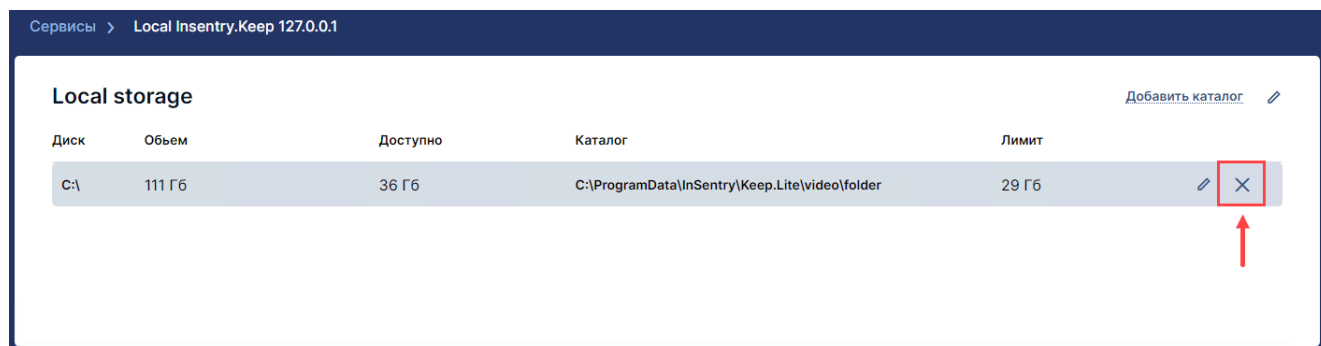
Local storage	
Диск	Режим записи
C:\	 Включена
Итого	

Добавить каталог

Укажите новое название.

Удаление каталога из хранилища

Чтобы удалить каталог, нажмите на кнопку удаления  в конце строки.



При удалении каталога запись в каталог прекращается, но папка и данные в ней не удаляются.

Изменение лимита записи

Чтобы изменить лимит записи, наведите курсор на строку правила записи и нажмите кнопку **Редактировать**  в конце строки.

Изменить запись потока

Local storage, 1920×1080@25fps, H264

Лимит (суток)

Отмена

Сохранить

Укажите новое значение лимита и нажмите кнопку **Сохранить**.

Настройка количества камер для записи архива

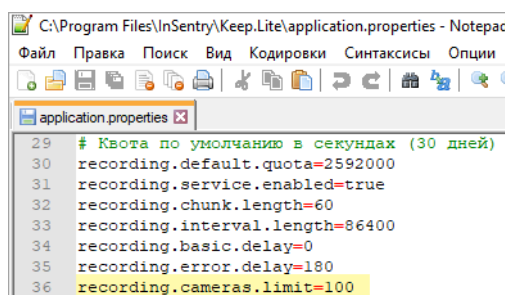
По умолчанию одновременно вести запись могут не более 100 камер. Максимальное количество камер определяется лицензией.

Значение можно изменить. Для этого в файле конфигурации модуля Keep укажите нужное количество в строке `recording.cameras.limit`, например: `recording.cameras.limit=170`.

Расположение файла конфигурации:

- в Linux: `/usr/src/InSentry/Keep.Lite/application.properties`
- в Windows: `C:\Program Files\InSentry\Keep.Lite\application.properties`

Указанное значение не должно превышать максимально допустимого лицензией, не рекомендуется указывать более 300.



Для применения изменённых настроек нужно перезапустить службу Keep.

Репликация архива. Иерархия модулей InSentry

Репликация архива применяется для отказоустойчивости и централизованного просмотра архива с большого количества камер.

Для настройки репликации создаются отдельные инсталляции InSentry, одна из инсталляций — основная (родительская), остальные — дочерние. Между модулями Watch в родительской и дочерней инсталляции настраивается иерархическая связь. Дочернему модулю даётся разрешение на запись архива в файлы родительской инсталляции, что позволяет заполнить возможные пробелы в записях архива основной инсталляции.

Ниже расскажем, как это настроить.

1. В основной и дочерней инсталляциях отредактируйте файл конфигурации `application.properties` модуля Watch, указав следующие значения:

```
modules.register.subnet=*
watch.host=10.10.10.10
insentry.link.enabled=true
```

Вместо 10.10.10.10 укажите внешний IP адрес сервера, на котором производится настройка: для дочерней инсталляции — адрес дочернего сервера, для родительской инсталляции — адрес основного сервера.

В инсталляции на линуксе все файлы создаются внутри контейнера. Перейдите внутрь контейнера командой `docker exec -it имя_контейнера bash` выполняйте действия с файлом `application.properties` уже внутри него. Полный путь до модулей внутри контейнера — `/usr/src/InSentry`. Директории, внутри которых лежат файлы конфигурации модулей, называются так же, как модули: Cast, Keep, Watch. Используйте команду `nano` имя_директории/`application.properties` для редактирования или создания файлов конфигурации.

Расположение файла конфигурации модуля Watch:

- Linux: `/usr/src/InSentry/Watch/application.properties`
- Windows: `C:\Program Files\InSentry\Watch.Lite\application.properties`

2. В основной и дочерней инсталляциях создайте новый файл `application.properties` для модуля Keep и укажите в нём следующие значения:

```
watch.host=10.10.10.10:9230
cast.host=10.10.10.10:5540
```

Вместо 10.10.10.10 укажите внешний IP адрес сервера, на котором производится настройка: для дочерней инсталляции — адрес дочернего сервера, для родительской инсталляции — адрес основного сервера. Порт оставьте без изменений.

Расположение файла конфигурации модуля Keep:

- Linux: `/usr/src/InSentry/Keep/application.properties`
- Windows: `C:\Program Files\InSentry\Keep.Lite\application.properties`

3. В основной и дочерней инсталляциях создайте новый файл `application.properties` для модуля Cast и укажите в нём внешний IP адрес сервера, на котором производится настройка. Порт оставьте без изменений.

```
watch.host=10.10.10.10:9230
```


Расположение файла конфигурации модуля Cast:

- Linux: /usr/src/InSentry/Cast/application.properties
- Windows: C:\Program Files\InSentry\Cast\application.properties

- В дочерней инсталляции в файле конфигурации application.properties модуля Keep укажите дополнительно следующие значения:

```
cloud.archive.host=20.20.20.20:3299
cloud.archive.bitrate=200
cloud.archive.chunklimit=30
cloud.archive.timegap=5
```

Вместо 20.20.20.20 укажите внешний IP адрес родительского сервера. Порт оставьте без изменений.

Расположение файла конфигурации модуля Keep:

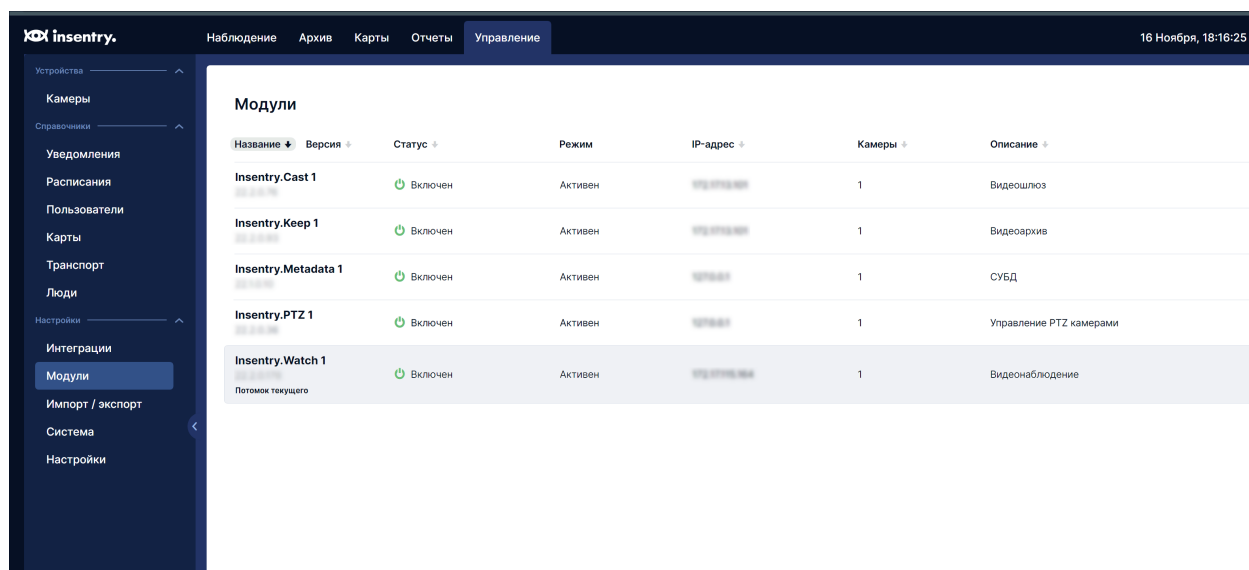
- Linux: /usr/src/InSentry/Keep/application.properties
- Windows: C:\Program Files\InSentry\Keep.Lite\application.properties

В основной инсталляции этого делать не нужно.

- В дочерней инсталляции перейдите в раздел **Управление → Модули** и нажмите кнопку **Добавить**.
- В открывшемся окне ручного добавления модуля укажите адрес и порт для подключения к серверу с основным модулем Watch. Порт по умолчанию: 9200.
- В дочерней инсталляции скачайте файл со списком камер и загрузите его в родительскую инсталляцию. Импорт и экспорт камер через файл производится в разделе **Управление → Импорт / экспорт**. Важно, чтобы все настройки камер в родительской и дочерней инсталляциях в точности совпадали.

См. также: [Импорт и экспорт камер через файл](#)

- В родительской инсталляции перейдите в раздел **Управление → Модули**.
- Если всё настроено правильно, то в списке появится дочерний модуль Watch. Перейдите в его настройки.



- Включите доверие модулю.

Настройки
Камеры

Insentry.Watch 1-потомок

Связь

Потомок текущего Watch

☒ Доверять модулю ?

☐ Доверять потомкам модуля, которым он сам доверяет ?

☒ Модуль доверяет текущему Watch ?

☒ Модуль доверяет родителю текущего Watch, если текущий Watch ему доверяет ?

Сохранить изменения

На этом настройка завершена. Теперь дочерний модуль Watch реплицирует пропущенные данные для записи в родительской инсталляции. Чтобы проверить работу репликации, отключите контейнер или службы Insentry.Keep и Insentry.Cast в родительской инсталляции на 10-15 минут и проверьте, что в родительской инсталляции в списке камер статусы камер зелёные, трансляция идёт и архив записывается.

Перед проверкой на всякий случай включите в дочерней инсталляции запись в архив критически важных данных с камер, чтобы ничего не потерять за время тестирования.

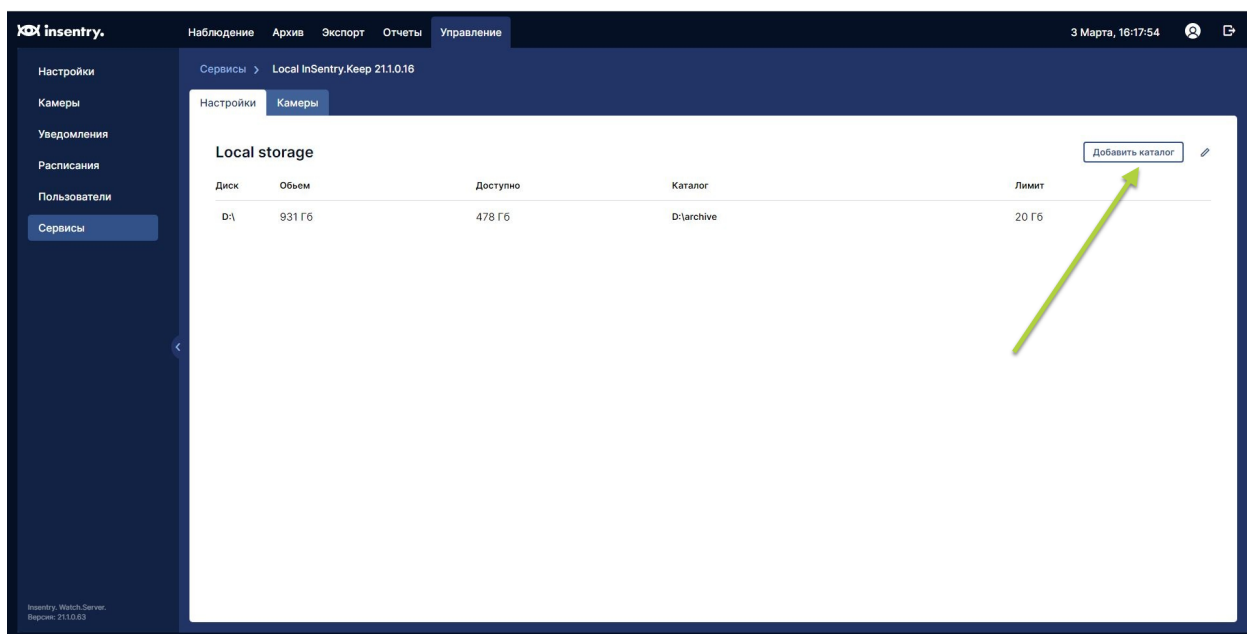
Перенос архива в другую папку или на другой носитель

Перед началом переноса:

- сделайте резервную копию переносимой папки на третьем носителе;
- убедитесь, что в целевой папке есть достаточного свободного места, чтобы сохранить лимит записи;
- убедитесь, что служба Insentry.Keep запущена.

Чтобы перенести архив видеозаписей с одного диска на другой без потери данных:

1. В разделе **Управление → Модули → Insentry.Keep** добавьте каталог с новой папкой. Если вы переносите архив уже в добавленный в Insentry каталог, то этот шаг можно пропустить.



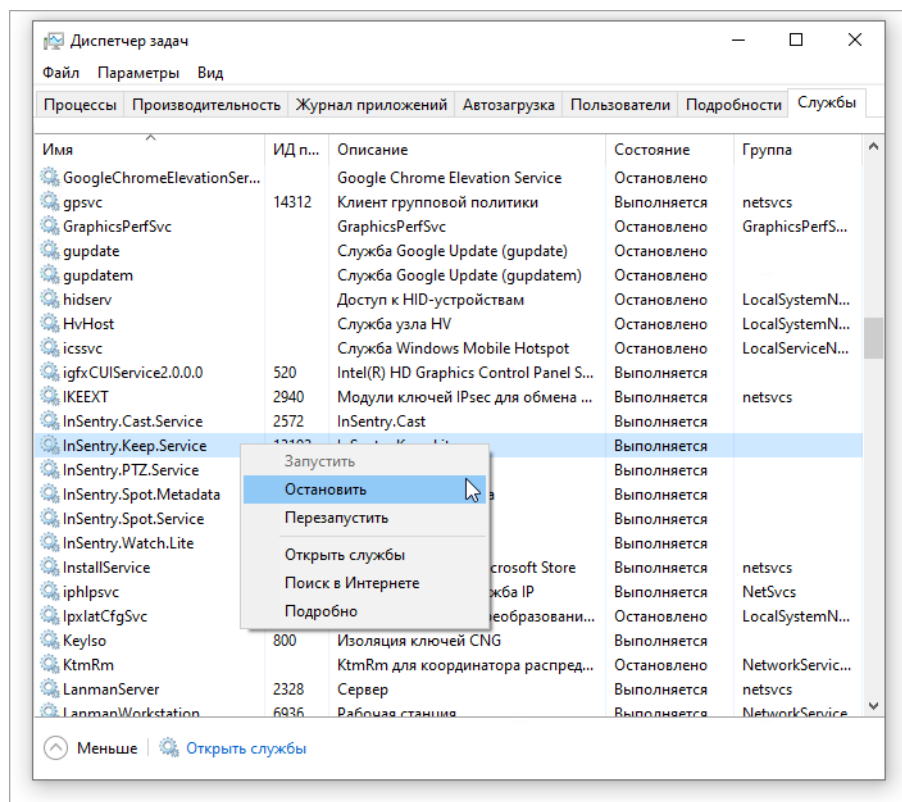
Добавить каталог

Диск: C: доступно 124 Гб из 669 Гб

Папка: videos

Лимит, Гб*: 40

2. Остановите службу **Insentry.Keep.Service** с помощью диспетчера задач.



3. Скопируйте папку **video** из старого хранилища в новое
4. В разделе **Управление** → **Модули** → **Local InSentry.Keep** **удалите** старую папку с архивом.
Если пропустить этот шаг, данные архива могут быть повреждены или утрачены.
5. Запустите службу InSentry.Keep.Service с помощью диспетчера задач.
6. Подождите пару минут для корректной индексации данных.
7. Проверьте целостность архива камеры во вкладке **Просмотр**.



Настройка модуля Spot

Модуль Spot отвечает за видеоаналитику и работу детекторов.

Нажмите на название модуля в **списке модулей** (**Управление** → **Модули**), чтобы перейти в настройке.

Камеры		Настройки		
Название	IP	Вендор / Модель	Потоки	Расположение
	1 1 172.17.17.17	Samsung Other PTZ-model	2 1	
	2 1 172.17.17.17	Polyvision Other PTZ-model	1 1	
	Test1 172.17.17.17	Vivotek FD8166A	1 3	
	Test 2 172.17.17.17 PTZ	Hikvision Other PTZ-model	3	
	Test3 172.17.17.17 PTZ	Axis P5515	1 1	

Список камер

На вкладке **Камеры** отображается список камер, на которых запущена видеоаналитика. Наведите курсор на статус работы детекторов, чтобы увидеть статистику их работы, как [в списке камер](#). По клику на название камеры вы можете перейти [к настройкам видеоаналитики](#) соответствующей камеры.

Настройки модуля

Во вкладке **Настройки** возможно переименовать модули и перевести его в режим обслуживания — он бывает нужен для диагностики работы модуля. В этом режиме служба Spot остаётся запущенной, но вся видеоаналитика отключается.

Камеры

Настройки

Модуль активен

☒

Режим обслуживания

Название*

InSentry.Spot 1

Описание

Видеоаналитика

Сохранить

Адрес для внешних подключений

Адрес и порты для передачи данных используются для работы пуш-уведомлений, Telegram бота, ссылок на события и передачи данных во внешние системы. По умолчанию в качестве внешнего

адреса будет использоваться адрес сервера.

Настройка производится в разделе **Управление → Система → Адрес для внешних подключений**.

Адрес для внешних подключений

Укажите адрес и порты, по которым сервер Insentry будет доступен из внешних систем. Эти настройки будут использоваться для формирования внешних ссылок.

☐ Введите IP адрес или hostname

☒ 172.18.249.252

☐ 172.17.13.23

Порт приложения используется для работы push-уведомлений, телеграм-бота и формирования ссылок на события и архив.

Переопределение порта

Протокол
 HTTP

Порт RTSP используется для передачи потоков по протоколу RTSP из Insentry во внешние системы и формирования ссылок на видеопотоки для ЕЦХД.

Переопределение порта RTSP

Сохранить

Импорт и экспорт камер

Список камер с настройками можно выгрузить в виде файла *.xlsx.

Импорт камер в Insentry

Импорт производится в разделе **Управление → Система → Импорт/Экспорт → Импорт конфигурации Insentry**. Там же можно скачать шаблон для заполнения списка камер.

Для импорта требуется файл *.xlsx с листами Cameras, Profiles и Recordings. Первые строки листов содержат названия столбцов и не парсятся при импорте, поэтому названия колонок могут быть любыми.

Формат листа Cameras

На листе Cameras обязательные для заполнения столбцы:

- Name
- Host
- Login

Если хотя бы один из них не заполнен, вся строка будет считаться комментарием, а не информацией о камере.

Остальные столбцы заполнять необязательно. Пустые столбцы будут интерпретироваться со значениями по умолчанию.

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Name	Название камеры	Текстовое поле длиной от 1 до 250 символов. Допустимы символы кириллицы, все печатные символы ASCII	Поле обязательно для заполнения
Host	Адрес камеры	IPv4 адрес или доменное имя камеры, порт — целое число от 1 до 65535, согласно спецификации	Поле обязательно для заполнения
Login	Логин доступа к камере	От 1 до 50 символов, допустимы все печатные символы ASCII	Поле обязательно для заполнения
Password	Пароль доступа к камере	От 1 до 50 символов, допустимы все печатные символы ASCII	Null
Description	Описание камеры	Текстовое поле длиной от 0 до 250 символов. Допустимы символы кириллицы, все печатные символы ASCII	Null
Vendor	Производитель камеры	Текстовое поле, значение должно содержать название одного из [поддерживаемых вендоров либо значение Other	Onvif]
Model	Модель камеры	Модель камеры. Если модель неизвестна, напишите Other model или Other PTZ-model	
Channel	Канал (для импорта камер с регистратора)	Целое число	Null
PTZ support	Идентификатор поворотной камеры	1 — да, 0 — нет	0
Use TCP	Если переключатель включен, то для получения потоков используется протокол TCP	1 — использовать TCP, 0 — использовать UDP	0
RTSP-port	Номер порта для передачи данных по протоколу RTSP	Целое число от 1 до 65535, согласно спецификации	554
HTTP-port	Номер порта для передачи данных по протоколу HTTP	Целое число от 1 до 65535, согласно спецификации	80
Onvif-port	Номер порта для передачи данных по протоколу Onvif	Целое число от 1 до 65535, согласно спецификации	80

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Profiles set	Идентификатор набора профилей	Указанный в листе Profiles либо пустой	Null
Recordings set	Ссылка на идентификатор набора записей в листе Recordings	Указанный в листе Recordings либо пустой	Null
UUID	Уникальный идентификатор UUID, который записывается в логах работы системы. Может пригодиться при обращении в техподдержку	Согласно спецификации . Если UUID задан и камера с таким UUID уже есть, то её настройки будут обновлены	Будет сгенерирован новый UUID
ECHDID	Числовой идентификатор камеры в ЕЦХД. Если значение задано, то на камере включается [трансляция в ЕЦХД]	Целое число	Null
Stream to the cloud	Включение трансляции в облако	1 — вкл, 0 — выкл	0
Location	Расположение камеры	Текстовая строка	Null
Location Lat	Координаты камеры — широта	Градусы от -90.0 до 90.0 в виде десятичной дроби. Разделитель — точка	Null
Location Lon	Координаты камеры — долгота	Градусы от -180.0 до 180.0 в виде десятичной дроби. Разделитель - точка	Null
direction	Направление объектива камеры в градусах	Значение от 0 до 359, где 0° — на восток, 90° — на север, 180° — на запад, 270° — на юг	Null

Если на листе Cameras хотя бы у одной камеры заполнен столбец «Набор профилей», то в файле импорта обязательно должны быть описания этих наборов в листе Profiles.

Если на листе Cameras хотя бы у одной камеры заполнен столбец «Recordings set», то в файле импорта обязательно должны быть описания этих наборов в листе Recordings.

Если на листе в Cameras задан UUID камеры и камера с таким идентификатором уже существует в базе. В этом случае:

1. Согласно листу Recordings добавляются правила записи по тем профилям камеры, по которым они отсутствуют.
2. По тем профилям, для которых уже существуют правила записи и для которых на листе Recordings найдена соответствующая запись, в существующих правилах записи обновляется глубина хранения и режим записи (включена или выключена).
3. Удаляются правила записи по тем профилям камеры, для которых отсутствует информация на листе Recordings (только в том случае, если на вкладке Cameras для камеры задан Recording set).

Формат листа Profiles

На листе Profiles обязательные столбцы:

- Profiles set
- Name
- RTSP-url

Если хотя бы один из них не заполнен, строка будет считаться комментарием.

Остальные столбцы заполнять необязательно. Пустые столбцы будут интерпретироваться со значениями по умолчанию.

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Profiles set	Идентификатор набора профилей	Целое число от 0 до 2 миллиардов	Поле обязательно для заполнения
Name	Название профиля	Строка, только латинские символы, нижнее подчёркивание и дефис, максимальная длина 64 символа	Поле обязательно для заполнения
RTSP-url	URL-путь для получения видеопотока по протоколу RTSP	URL-путь	Поле обязательно для заполнения
Screen-url	URL-путь для получения скриншотов с камеры по протоколу HTTP	URL-путь	Null
Codec	Название кодека	Строка не чувствительная к регистру, поддерживается только кодек H264	Null
Width	Ширина потока	Целое число от 64 до 16384	Null
Height	Высота потока	Целое число от 64 до 16384	Null
FPS	FPS потока	Целое число от 0 до 1000	Null

Формат листа Recodrings

На листе Recordings обязательные для заполнения столбцы:

- Recording set
- Depth
- Enabled
- Width и Height либо Profile

Если хотя бы один из них не заполнен, вся строка будет считаться комментарием.

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Recording set	Идентификатор набора записей	Целое число	Поле обязательно для заполнения
Depth	Глубина хранения архива в днях	Целое или дробное число	Поле обязательно для заполнения

Столбец	Описание	Формат	Значение по умолчанию, если ячейка не заполнена
Enabled	Статус записи	1 — запись включена, 0 — выключена	Поле обязательно для заполнения
Width	Ширина видеопотока (может отсутствовать, если указан Profile)	Целое число от 64 до 16384	Поле обязательно для заполнения, если не заполнено поле Profile
Height	Высота видеопотока (может отсутствовать, если указан Profile)	Целое число от 64 до 16384	Поле обязательно для заполнения, если не заполнено поле Profile
Profile	Идентификатор профиля видеопотока (может отсутствовать, если заданы значения Width и Height). Если указан Profile — проверяется его существование у камеры и правило записи создается с этим профилем. Если Profile не указан или у камеры нет такого профиля, а Width и Height не указаны — импорт камеры не производится	Целое число	Поле обязательно для заполнения, если не заполнены Width и Height

Если Profile не указан или потока с таким профилем на камере нет, то при импорте проверяется наличие правил записи потока по значениям ширины и высоты. Если правило записи для такого потока с таким разрешением уже создано, новое правило при импорте не создаётся.

Экспорт списка камер и настроек

Экспорт производится в разделе **Управление → Система → Импорт/Экспорт → Экспорт конфигурации Insentry**. При экспорте выгружается файл со списком и настройками камер. Формат файла такой же, как для импорта.

Экспорт списка камер для ЕЦХД

Скачать список камер в формате, подходящем для ЕЦХД, можно в разделе **Управление → Подключения → ЕЦХД**, во вкладке **Список камер**.

См. также: [Настройка интеграции с ЕЦХД](#)

Удаление всех камер

в разделе **Управление → Система → Импорт/Экспорт → Удаление всех камер** можно удалить все камеры и стереть записанный архив. Будьте внимательны, после удаления архив невозможно восстановить.

Работа с лицензиями

Лицензии позволяют использовать ПО Insentry, установленное на вашем компьютере или сервере.

ПО Insentry выпускается в трёх редакциях: [Free](#), [Standard](#), [Professional](#). Редакции различаются по максимальному количеству подключенных камер и физических серверов, на которых размещается ПО Insentry, а также по функционалу. На один аккаунт Insentry можно зарегистрировать только одну лицензию Free.

Начиная с версии 23.4, оформить лицензию на ПО Insentry можно на портале [insentry.video](#). Чтобы использовать бесплатную редакцию Insentry, нужно активировать бесплатную лицензию.

Если вы использовали бесплатную редакцию ПО Insentry версии 23.3 и ниже, после обновления на версию 23.4 вам будет предложено активировать лицензию (раньше активировать бесплатную лицензию было необязательно). Зарегистрируйтесь на портале [insentry.video](#) и выберите бесплатную лицензию. После этого скопируйте полученный ключ лицензии и активируйте его в веб-клиенте Insentry, доступном по адресу сервера. После этого вы сможете продолжить работу с ПО Insentry в обычном режиме.

Ключи бывают двух типов:

- ключ лицензии — нужен для того, чтобы активировать лицензию на редакцию ПО Insentry,
- ключ расширения — позволяет добавить в ПО Insentry новые камеры.

Активация ключей производится на сервере, где установлено ПО Insentry, в офлайн или онлайн режимах.

Чтобы посмотреть информацию об используемой лицензии, активировать лицензию или ключ расширения, перейдите в раздел **Управление → Система → Информация о лицензиях**.

Внимание! После подключения новых камер обязательно нужно активировать лицензию заново.

Выбор и покупка лицензии

Чтобы увидеть доступные лицензии, зарегистрируйтесь на сайте [insentry.video](#). На стартовом экране после регистрации будет предложено выбрать лицензию.

В магазине лицензий просмотрите описания лицензий и выберите подходящую. Бесплатную лицензию не нужно покупать — она только активируется. Платные лицензии можно оплатить в корзине. Оплата картой производится через Робокасса сразу же. Если выбрать оплату по счёту, то после оформления заказа на почту, указанную при регистрации, придёт письмо с реквизитами для оплаты. Письмо приходит не сразу, а после выставления счёта.

Добавьте лицензию или нужное количество ключей расширения в корзину и оплатите заказ с помощью карты или по счёту. После оформления заказа на почту приходит письмо с ключом. Если письмо не пришло, сообщите в техподдержку по адресу support@insentry.io.

Просмотреть информацию о действующей лицензии и скопировать ключ можно в разделе **Личный кабинет → Мои лицензии**.

Созданные заказы можно увидеть в разделе **Личный кабинет → Магазин лицензий → Мои заказы**.

После покупки лицензию нужно активировать.

Активация лицензии

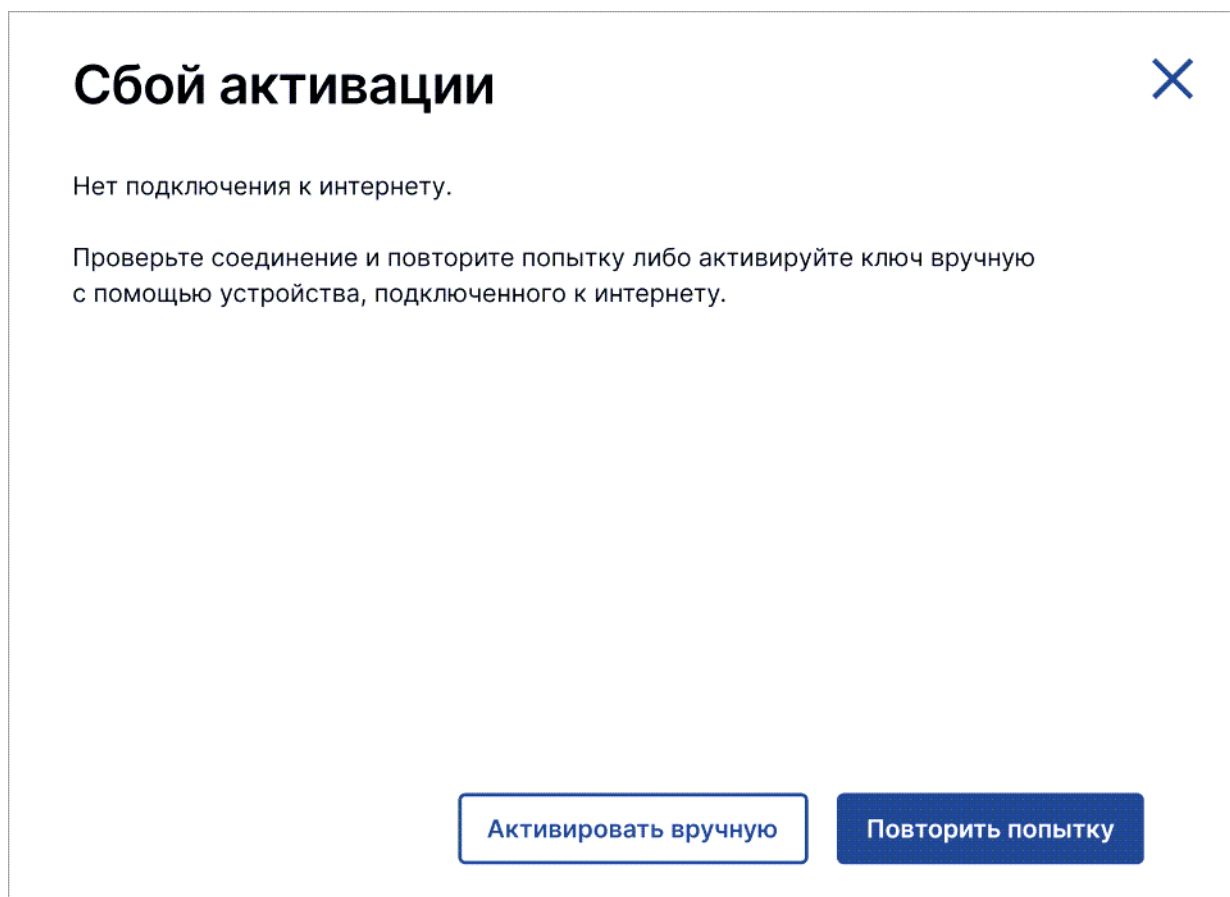
Онлайн активация

Чтобы активировать лицензию:

1. Скопируйте ключ лицензии из письма, которое пришло на почту после регистрации, или скопируйте его в разделе **Личный кабинет → Мои лицензии** на сайте insentry.video.
2. Авторизуйтесь под учётной записью администратора в веб-клиенте Insentry, запущенном на вашем сервере или компьютере.
3. Укажите ключ лицензии в разделе **Управление → Система → Информация о лицензиях**. При первом запуске веб-клиента Insentry указать ключ лицензии потребуется для начала работы с системой, и на стартовом экране вы увидите инструкции о том, как это сделать.

Если всё прошло успешно, на экране будет представлена [информация о лицензиях](#).

Если в процессе активации произойдёт сбой подключения, будет представлено следующее окно:



В этом случае проверьте подключение и повторите попытку, либо активируйте лицензию вручную.

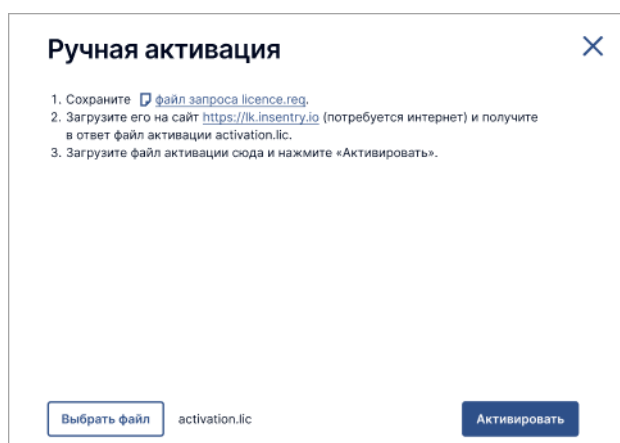
В дальнейшем управлять лицензиями можно в разделе **Управление → Система → Информация о лицензиях**.

Офлайн активация

Этот способ подходит для активации лицензии на сервере, не подключенном к интернету.

Перейдите в раздел **Управление → Система → Информация о лицензиях**.

На начальном экране нажмите **Активировать ключ**, укажите данные о лицензии и нажмите кнопку **Активировать**. Онлайн-активация не завершится, потому что нет подключения к интернету. Тогда нажмите кнопку **Активировать вручную**.



Чтобы активировать лицензию вручную:

1. Сохраните файл запроса *licence.req*.
2. Перенесите его на любой компьютер, подключенный к интернету.
3. Загрузите файл на сайт <https://lk.insentry.io/>. В ответ будет загружен файл активации *activation.lic*.
4. Сохраните файл *activation.lic* и перенесите его на сервер, куда будет установлено ПО Insentry.
5. Загрузите файл *activation.lic* и нажмите **Активировать**.

Файл активации можно использовать в дальнейшем для повторной активации лицензии, если потребуется — например, после добавления новых камер.

Расширение лицензии

Расширение лицензии нужно, чтобы добавить новые камеры без изменения редакции. Если вы собираетесь сменить редакцию Insentry, то удалите лицензию и затем активируйте новый ключ лицензии.

Чтобы расширить лицензию и добавить в Insentry новые камеры, требуется ключ расширения.

Чтобы добавить ключ расширения:

1. Купите ключ расширения на сайте insentry.video.
2. В веб-интерфейсе ПО Insentry перейдите в раздел **Система → Информация о лицензиях**.

Система > Информация о лицензии

Вы используете редакцию Standard

Удалить лицензию Расширить лицензию Магазин лицензий

Данные о лицензии	В лицензии	Активировано	Ожидает активации
Камеры	16	7	0
Серверы	1	1	

Ключ Тип

Ключ лицензии

- Нажмите кнопку **Расширить лицензию**.
- Укажите ключ расширения и нажмите **Активировать**.

Ключ расширения лицензии

Если вы хотите активировать ключ другой лицензии, то удалите текущую лицензию и после этого активируйте новый ключ.

Ключ расширения лицензии
f69117ae-b68d-c3ef-e83f-64d81791d269

Активировать

Удаление лицензии

Чтобы перенести Insentry на другой сервер или сменить редакцию, удалите лицензию и активируйте её заново после переноса.

При удалении лицензии редакция Insentry сбрасывается до базовой: все функции Insentry продолжают работать только на первых 16 добавленных камерах.



Удалить лицензию?

Лицензия будет сброшена до базовой редакции Standard. Видеоаналитика, запись архива и наблюдение продолжат работать на первых 16 добавленных камерах.

Отмена

Да

Перевыпуск ключа

При переносе ключа на другую систему, а также при переустановке ПО Insentry после форматирования системы старый ключ активации не может быть повторно активирован. Для таких случаев нужен перевыпуск ключа.

После перевыпуска ключа старый ключ отзывается — видеонаблюдение, видеоаналитика и архив на камерах, добавленных по лицензии со старым ключом, сразу же перестанут работать.

Новый ключ лицензии будет показан в информации о лицензии в разделе **Личный кабинет** → **Мои лицензии** на сайте insentry.video.

Перевыпуск ключа доступен не чаще, чем раз в три дня.

Передача данных в облако Insentry Cloud

В разделе **Управление** → **Система** → **Insentry Cloud** можно связать серверную инсталляцию Insentry с [облаком Insentry](https://insentry.video), чтобы видео и архив камер, подключенных к серверной версии Insentry, отображались в облаке.

Выполните действия в следующем порядке:

1. Оформите подписку на сайте insentry.video. Бесплатная версия позволит просматривать в реальном времени 60 минут видео в сутки с каждой камеры. В платной версии можно смотреть видео в реальном времени без ограничений, а также записывать и просматривать архив.
2. Включите передачу данных в облако из серверной версии в разделе **Управление** → **Система** → **Insentry Cloud**.
3. Дождитесь, пока подключение перейдёт в статус «Подключено».
4. Скопируйте серийный номер и введите его в разделе **Управление** → **Insentry.Bridge** на сайте insentry.video.

5. В серверной инсталляции включите трансляцию данных в облако **в настройках камер**, которые вы хотите транслировать. Если в настройках трансляция в облако отключена, а в системных настройках включена, камера не будет транслировать данные в облако. Но если в системных настройках трансляция выключена, то включение трансляции в настройках камеры не повлияет на передачу данных — она останется отключенной.
6. Подождите несколько минут, чтобы соединение установилось. Проверьте, что всё работает корректно:
 - в разделе **Управление → Система → Insentry Cloud** статус подключения должен быть «Подключено»;
 - в облаке Insentry на сайте insentry.video должны отображаться нужные камеры из серверной инсталляции.

При отключении передачи данных на сервере, ранее подключенные к облаку камеры не удаляются из облака, так как на них может быть записан архив. Чтобы удалить камеры из облака, зайдите в настройки камер на облаке на портале insentry.video.

Прочие настройки

Доступ к локальному серверу Insentry из WAN сети (проброс портов)

Чтобы обеспечить доступ из сети Интернет к локальному серверу Insentry:

1. Узнайте внешний IP адрес вашего роутера на сайте <http://2ip.ru/>.
2. Определите модель роутера.
3. Настройте проброс портов как указано в инструкции к вашему роутеру.
4. Проверьте настройки брандмауэра/фаерволла, создайте правила и откройте требуемые порты.

Каждый из портов нужен для работы определённого модуля: Cast, Keep, Watch, Spot, PTZ.

Обязательно должны быть открыты порты двух модулей: Watch (модуль, отвечающий за клиент Insentry) и Cast (модуль, отвечающий за live-трансляцию с камер). Строки с описанием этих модулей отмечены жирным шрифтом.

Если какой-то из модулей Keep, Spot и PTZ в вашей системе не используется, то нет необходимости открывать порты из указанной группы и создавать дополнительные правила.

Порт	Протокол	Модуль	Описание
3301	TCP	Cast	Порт трансляции видео (Websocket)
3291	TCP	Keep	Порт трансляции видео из архива (Websocket)
3297	TCP	Keep	Порт трансляции видео из архива (RTSP)
3299	TCP	Keep	Порт управления службой видеоархива (HTTP)
5540	TCP	Cast	Порт для трансляции видео (RTSP)
9200	TCP	Watch	Порт тонкого клиента и интерфейса администратора Watch
7560	TCP	Spot	Внутренний порт службы видеоаналитики (Stomp)
8008	TCP	PTZ	Порт управления службой поворота камер (Http)
8520	TCP	Spot	Порт управления службой видеоаналитики (HTTP)
8530	TCP	Spot	Порт для взаимодействия со службой метаданных видеоаналитики
8535	TCP	Spot	Внутренний порт службы метаданных видеоаналитики
9350	TCP	Cast	Порт управления службой ретрансляции видео (HTTP)

Порт	Протокол	Модуль	Описание
8081	TCP	Spot	Порт службы MessageBroker

Инструкции по настройке правил проброса портов для самых распространенных моделей роутеров:

- [Mikrotik](#)
- [TP-LINK](#)
- [D-LINK](#)
- [ASUS](#)
- [XIAOMI](#)

Настройка HTTPS соединения

Для настройки HTTPS соединения с сервером Insentry воспользуйтесь сервером Caddy. После установки и настройки сервера Caddy, он автоматически получит SSL сертификат и будет его обновлять с помощью сервиса Let's Encrypt.

Установка Caddy для Ubuntu 20.04

1. Убедитесь, что все ваши системные пакеты обновлены:

```
sudo apt update && sudo apt upgrade
```

2. Установите сервер Caddy:

```
sudo apt install -y debian-keyring debian-archive-keyring apt-transport-https
&& \
curl -1sLf 'https://dl.cloudsmith.io/public/caddy/stable/gpg.key' | sudo gpg
--dearmor -o /usr/share/keyrings/caddy-stable-archive-keyring.gpg && \
curl -1sLf 'https://dl.cloudsmith.io/public/caddy/stable/debian.deb.txt' | sudo
tee /etc/apt/sources.list.d/caddy-stable.list && \
sudo apt update && \
sudo apt install caddy
```

3. Откройте для редактирования конфигурационный файл Caddy:

```
sudo nano /etc/caddy/Caddyfile
```

4. Отредактируйте конфигурационный файл Caddy в соответствии с образцом, замените блоки в квадратных скобках на IP и доменное имя вашего сервера:

```
# The Caddyfile is an easy way to configure your Caddy web server.
#
# Unless the file starts with a global options block, the first
# uncommented line is always the address of your site.
#
# To use your own domain name (with automatic HTTPS), first make
# sure your domain's A/AAAA DNS records are properly pointed to
# this machine's public IP, then replace ":80" below with your
# domain name.
```

```
https://[Доменное имя вашего сервера] {
    reverse_proxy localhost:9200
```

```

}

http://[IP адрес вашего сервера] {
    reverse_proxy localhost:9200
}

# Refer to the Caddy docs for more information:
# https://caddyserver.com/docs/caddyfile

```

5. Запустите сервер Caddy и проверьте его статус:

```
sudo systemctl start caddy && sudo systemctl status caddy
```

Воспроизведение потока на сайте через NPM плеер

Чтобы выводить видеопоток с настроенной видеоаналитикой Insentry на свой сайт через NPM плеер, нужно авторизоваться в API и получить токен и URL, по которым доступны службы Insentry. Токен присваивается автоматически при авторизации на сервере Watch.

Для запуска плеера потребуются значения следующих элементов API:

- **userToken** — токен для авторизации,
- **spotUrl** — адрес для подключения к службе Spot,
- **liveUrl** — адрес для трансляции видео с камеры,
- **cameraId** — идентификатор камеры.

Каждый запрос подписан токеном. Токен становится недействительным через три часа, если по нему не было запросов. Если токен недействителен, то API иницирует на своей стороне переподключение с новым токеном. Лучшее решение — регулярно запрашивать статус, чтобы работать через один токен без переподключения.

Установка плеера

Для установки плеера через NPM-репозиторий используется команда:

```
npm install web-video-player
```

Если репозиторий недоступен, то можно установить плеер офлайн. Для этого [скачайте артефакт](#) и положите его в папку проекта, после этого установите плеер командой:

```
npm install web-video-player@21.1.11.tgz
```

Внедрение видеоплеера в React приложении

1. Импортируйте React и VideoPlayer:

```
import React from 'react';
import VideoPlayer from 'web-video-player';
```

2. Передайте с помощью элемента **props** необходимые для запуска плеера зависимости:

```

<VideoPlayer
  sync={boolean}
  debug={boolean}
  sceneInfo={Array}
  spot={function}
  spotUrl={string}
  className={string}
  onPlay={function}
  onError={function}
  cameraId={string}
  userToken={string}
  liveUrl={string}
  width={number}
  height={number}
/>

```

- Для показа видеоаналитики импортируйте объект с подключением к Spot службе и настройте его взаимодействие с плеером:

```

import { SpotConnection } from 'web-video-player';
const spotConnection = new SpotConnection(spotUrl, errorCallback,
  successCallback)

```

где `spotConnection` — функция, которую необходимо передать плееру в качестве `spot` prop.

- Потом во время рендера передайте инстанс `spotConnection` плееру в качестве `spot` prop:

```

<VideoPlayer {...otherProps} spot={spotConnection} />

```

- Для показа видеоаналитики с локализованным текстом передайте массив с расшифровкой параметров аналитики в `sceneInfo` prop:

```

<VideoPlayer {...otherProps} sceneInfo={/* Массив с переводами сообщений от
  детекторов */} />

```

- Для авторизации в службах Spot и Cast используется токен,. Так же для подключения необходимо передать UUID камеры, который ей присвоил Watch:

```

<VideoPlayer {...otherProps} userToken={/* токен пользователя */}
  cameraId={/* UUID камеры */} />

```

Токен можно получить из `localStorage` или из заголовка запроса к серверу.

Name	Value
login	
login	
detectors	
api.amplitude.com	
layouts	
cameras	
menu	
cameras	
models	
modules	
status	
status?last=1612447206289&wait=60	
ec75621d-ba39-424b-adf6-edcbe1a80214	
scene	
status?last=1612447206289&wait=60	
status?last=1612447206289&wait=60	

General
Request URL: http://localhost:9200/api/webclient/login
Request Method: POST
Status Code: 200
Remote Address: [::1]:9200
Referrer Policy: strict-origin-when-cross-origin

Response Headers
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Type: application/json; charset=UTF-8
Date: Fri, 05 Feb 2021 09:06:56 GMT
Expires: 0
Pragma: no-cache
Transfer-Encoding: chunked
X-Content-Type-Options: nosniff
X-User-Token: ee64edcd-9c97-4af5-a06c-1ebde94aa005
X-XSS-Protection: 1; mode=block

7. Адреса служб Cast и Spot можно получить из localStorage или сформировать их самостоятельно `ws://{host}:{port}/{serviceName}`

Если авторизация прошла успешно, то номера портов служб приходят в ответе на запрос авторизации в формате JSON: `api/webclient/login`.

Так же в localStorage можно узнать токен пользователя — `/api/webclient/login`
`/api/webclient/login /api/api/webclient/login/webclient/login`

Name	Headers	Preview	Response	Initiator	Timing	Cookies
login						
login			<pre>{ "userName": "Admin", "language": "RUS", "preview": "BIG", "fitMode": "FULL", "showNameMode": "ANYTIME", "instanceId": "cf522349-4e37-40e1-8ec7-8a522e85d1ae", "isAdmin": true, "language": "RUS", "message": null, "preview": "BIG", "servicePorts": { "castWS": 3301, "keepHttp": 3299, "keepWS": 3291, "spotWS": 8081 }, "showNameMode": "ANYTIME", "showNameStyle": "ALL", "status": "OK", "systemHash": "f2664f835193067c754426d52f268b20", "userName": "Admin", "version": "20.1.0.764" }</pre>			
detectors						
api.amplitude.com						
layouts						
cameras						
menu						
cameras						
models						
modules						
status						
status?last=1612447206289&wait=60						
ec75621d-ba39-424b-adf6-edcbe1a80214						
scene						

Application	Filter	Key	Value
Manifest			
Service Workers			
Storage			
Storage			
Local Storage			
http://demo.insentry.io:920			
Session Storage			
IndexedDB			
Web SQL			
Cookies			
Cache			
Cache Storage			
Application Cache			
Background Services			
Background Fetch			
Background Sync			
Notifications			
Payment Handler			
		Key	Value
		demo.insentry.io_web-client-current-shownamemode	ANYTIME
		SPOT	ws://demo.insentry.io:8081/spot
		demo.insentry.io_web-client-current-name	Admin
		demo.insentry.io_web-client-current-login	Admin
		demo.insentry.io_web-client-current-preview	BIG
		amplitude_unsent_identify_ed3562f3606eb2a43b89bb0fd805057f	
		KEEP	ws://demo.insentry.io:3291/archive
		demo.insentry.io_web-client-current-format	FULL
		demo.insentry.io_web-client-current-shownamestyle	ALL
		demo.insentry.io_web-client-current-clientip	192.168.89.1
		PTZ	ws://demo.insentry.io:8008/api/ptz
		_revision	21.1.0.818
		undefined_web_cli_state	
		amplitude_unsent_ed3562f3606eb2a43b89bb0fd805057f	
		CAST	ws://demo.insentry.io:3301/live
		demo.insentry.io_web-client-current-id	7a638366-5505-41e1-9a46-b1304aa17464
		demo.insentry.io_web-client-current-token	02105427-97cd-49b1-8a74-c6dd0a06c3fc
		demo.insentry.io_web-client-current-systemhash	16b16c141a95cecb3eab5cad4c620798
		demo.insentry.io_web-client-current-isAdmin	true
		demo.insentry.io_web-client-current-plugins	["webClientPlugin"]

```
<VideoPlayer {...otherProps} liveUrl="ws://demo.insentry.io:3301/live"
spotUrl="ws://demo.insentry.io:8081/spot" />
```

Дополнительные параметры:

Параметр	Описание	Обязательный
width	Ширина окна плеера	Да
height	Высота окна плеера	Да
onPlay	Функция коллбек, будет вызвана после получения и воспроизведения видеопотока	Да
onError	Функция коллбек, будет вызвана после неудачной попытки начать воспроизведение видеопотока	Да
class-	Дополнительный класс для кастомизации плеера	Нет
Name		
sync	Выключает синхронизацию аналитики от Spot и видео с Cast службы. Значение по умолчанию — true	Нет

Параметр	Описание	Обязательный
debug	Режим дебага аналитики и воспроизведения видеопотока. Если он включен, то логируется дополнительная информации в консоль браузера и добавляется отображение времени воспроизведения и аналитики в режиме реального времени. Значение по умолчанию — <code>false</code>	Нет

Получение событий видеоаналитики

Ниже приведены примеры того, каким образом можно получать события видеоаналитики Insentry. Для настройки получения событий видеоаналитики Insentry в вашем проекте напишите запрос на support@insentry.io.

Получение данных через web-stomp

Тонкий клиент взаимодействует со службой Spot для:

- получения информации о событиях видеоаналитики в реальном времени,
- получения информации о тревогах, выявленных [детекторами видеоаналитики](#),
- доступа к архиву событий видеоаналитики.

Для подключения к через STOMP используется URL `ws://HOST:PORT/spot`, где:

- **HOST** - адрес службы InSentry.Spot
- **PORT** - порт службы InSentry.Spot (обычно 8081)

Взаимодействие тонкого клиента со службой Spot.Lite ведется [по протоколу STOMP](#), работающему поверх протокола WebSocket.

Получение событий в реальном времени

Для получения событий видеоаналитики в реальном времени тонкий клиент подписывается на топик, выполняя STOMP-запрос **SUBSCRIBE**:

```
/topic/[camera_id]/[detector_id]
```

где:

- `camera_id` — идентификатор камеры в формате GUID
- `detector_id` — идентификатор детектора, указанный в дескрипторе kernel (Формат дескриптора Kernel) в поле `$.detectors[*].id`

Например:

```
/topic/f0a72c41-79e2-4ba5-a894-6726c6f5358b/motionDetector
```

Для подписки на события сразу с нескольких камер могут быть использованы маски, задаваемые символом `>` и означающие подписку на все субтопики. Например, для получения событий по камере `f0a72c41-79e2-4ba5-a894-6726c6f5358b` от любых детекторов необходимо подписаться на топик:

```
/topic/f0a72c41-79e2-4ba5-a894-6726c6f5358b/>
```

Для получения событий от любых детекторов с любых камер, обслуживаемых одной и той же службой Spot, необходимо подписаться на топик:

```
/topic/>
```

Получение состояния сцены и изменений состояния

После входу в систему тонкому клиенту необходимо получить информацию об изменениях состояния сцены, которые произошли до его подключения: состояние счетчиков, объекты разметки и т.д. Перед началом проигрывания архива, тонкому клиенту необходимо состояние сцены, которое сформировалось до того момента, с которого планируется начать просмотр архива.

Когда архив находится на паузе, при кликах по таймлайну в архиве тонкому клиенту необходимо состояние сцены на тот момент времени, для которого отображается скриншот в режиме паузы. Для получения этой информации тонкий клиент выполняет STOMP-запрос **SUBSCRIBE**:

```
/api/state/[camera_id]
```

Заголовки запроса: `frameTimestamp:[frameTimestamp]` где:

- `camera_id` — идентификатор камеры в формате GUID, состояние сцены по которой необходимо получить,
- `frameTimestamp` — момент времени, для которого необходимо получить текущее состояние сцены (unix-time в микросекундах). Параметр не обязательный и может отсутствовать, в этом случае возвращается состояние сцены на текущий момент времени.

Например:

```
/api/state/edc366f3-a80b-4d6e-a306-0946bef3e527
```

В ответ на подписку к этому топикю клиент получает сообщение, содержащее состояние сцены по каждому из детекторов в том же формате, как и в запросе получения информации из архива событий видеоаналитики.

Пример ответа от детектора

Пример ответа [детектора движения в запрещённой зоне](#):

```
content-type: application/json;charset=utf-8
content-length: 1237
cameraId: 8f05484c-7a79-41fd-9c71-ea4916a68b40
timestamp: 1531945640234
detectorId: faceDetector
eventType: sceneUpdate
frameWidth: 1024
frameHeight: 768
```

```
{
  "objects": [
    {
      "id": "91307ce9-332b-41a9-b53b-617a28c8b878",
      "action": "shot",
      "class": "motion",
      "points": [
        {
```

```

        "x": 100,
        "y": 120
    },
    {
        "x": 300,
        "y": 200
    }
],
"states": [
    {
        "id": "zone",
        "float": 0
    }
]
},
{
    "id": "3c4c0f95-476c-4291-a05f-f0f20c439475",
    "action": "shot",
    "class": "motion",
    "points": [
        {
            "x": 500,
            "y": 320
        },
        {
            "x": 600,
            "y": 420
        }
    ],
    "states": [
        {
            "id": "zone",
            "float": 1
        }
    ]
},
{
    "id": "4b29e160-c4e2-4172-9685-7fcfd51a10ac",
    "action": "shot",
    "class": "motion",
    "points": [
        {
            "x": 10,
            "y": 12
        }
    ],
    "states": [
        {
            "id": "zone",
            "float": 3
        }
    ]
}
]

```



Решение проблем

Система не обнаруживает камеру

Если ПО Insentry не может обнаружить камеру, необходимо провести диагностику сети по принципу «снизу вверх» согласно модели OSI.

Проверка физического уровня

В первую очередь проверьте:

- правильность подключения кабелей,
- наличие индикации на камере и маршрутизаторе, к которому подключена камера,
- наличие электропитания в зависимости от типа подключения камеры (адаптер, POE инжектор).

Если с коммутацией всё хорошо, питание на камере есть, индикация работающего подключения на маршрутизаторе мигает, а камера всё равно не подключается к ПО Insentry, то переходите ко второму уровню диагностики.

Проверка канального уровня

Зайдите на маршрутизатор любым доступным способом (через веб-интерфейс, telnet, ssh) и проверьте наличие на нём MAC-адреса камеры.

MAC-адрес имеет следующий формат: 00:26:57:00:1f:02. У большинства производителей камер MAC адрес написан на коробке от камеры либо на обратной стороне самой камеры.

Таблица, содержащая MAC-адреса и соответствующие им IP адреса, называется таблицей ARP записей. Эта таблица составляется из MAC-адресов видимых устройств и находится на маршрутизаторе. Пример ARP-записи:

IP-адрес	MAC-адрес	Тип
172.16.10.253	00:1C:C5:34:B3:01	Динамический
172.16.10.88	1C:75:08:D2:49:45	Статический

Если MAC-адрес камеры виден, то для дальнейшей диагностики запишите IP адрес, который соответствует MAC-адресу камеры, и переходите к следующему уровню диагностики.

Если MAC-адреса камеры нет в ARP-таблице на маршрутизаторе, то вернитесь к предыдущему уровню диагностики.

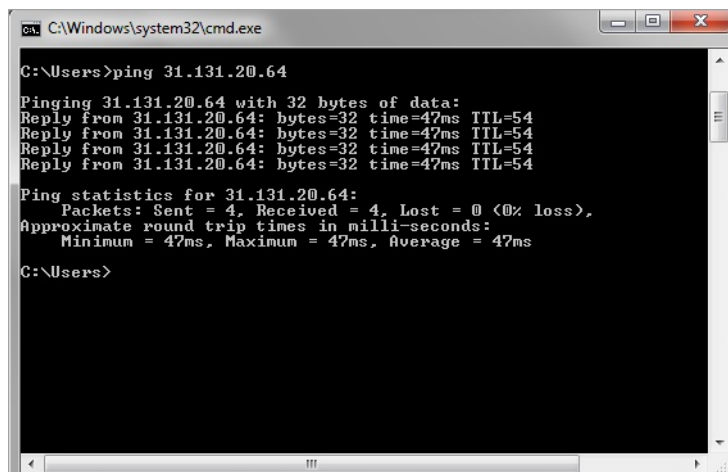
Проверка сетевого и транспортного уровней

Для проверки сетевой связности с камерой используйте команду ping:

- Для Windows: **Пуск → Выполнить → cmd → ping IP_адрес_камеры .**
- Для Linux: **Открыть терминал → ping IP_адрес_камеры .**

Эта команда отправляет серию эхо запросов для диагностики сетевой связности двух устройств.

Пример выполнения команды ping :



```

C:\Windows\system32\cmd.exe

C:\Users>ping 31.131.20.64

Pinging 31.131.20.64 with 32 bytes of data:
Reply from 31.131.20.64: bytes=32 time=47ms TTL=54
Reply from 31.131.20.64: bytes=32 time=47ms TTL=54
Reply from 31.131.20.64: bytes=32 time=47ms TTL=54
Reply from 31.131.20.64: bytes=32 time=47ms TTL=54

Ping statistics for 31.131.20.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 47ms, Maximum = 47ms, Average = 47ms

C:\Users>
  
```

Если ответа от камеры нет, повторите диагностику первого и второго уровней.

Если ответ получен, переходите к проверке прикладного уровня подключения.

Проверка прикладного уровня

Последний этап проверки — если MAC адрес камеры приходит и ping до камеры есть, то скорее всего камера будет обнаружена с помощью ПО Insentry.

В противном случае проверьте:

- доступность веб-интерфейса,
- логин и пароль для управления камерой,
- открыты ли порты для видеопотока — для этого используйте пакет telnet.

Для того чтобы попасть на веб-интерфейс камеры, укажите в адресной строке браузера IP адрес камеры в формате `http://10.10.10.10`. Если доступа к веб-интерфейсу камеры нет, сбросьте настройки камеры до заводских и настройте камеру заново. Если после сброса настроек веб-интерфейс всё ещё недоступен, обратитесь к производителю камеры для проверки её работоспособности.

Веб-интерфейсы камер работают нестабильно, и лучше всего для подключения к веб интерфейсу использовать браузер Internet Explorer.

Проверка с помощью ONVIF Device Manager

Чтобы проверить корректность настроек камеры для обнаружения по протоколу ONVIF:

1. Проверьте, что в настройках камеры указаны корректные вендор, модель камеры и порт ONVIF (он может быть нестандартным у некоторых камер).
2. Проверьте корректность настроек с помощью программы Onvif Device Manager.

Для обращения в техподдержку Чтобы специалисты техподдержки скорее смогли решить вашу проблему, заранее сделайте скриншоты со вкладок **Network settings**, **live video**, **video streaming**, **profiles** в программе Onvif Device Manager и приложите их при создании обращения.

Контакты техподдержки:

Телефон: +7 (495) 540-47-44

Почта: support@insentry.io

Телеграм: [@insentry_support](https://t.me/insentry_support)

Не записывается архив

В случае возникновения проблем с записью архива камеры:

1. Проверьте работоспособность жесткого диска или локального хранилища и сервера, на котором ведется запись архива. Посмотреть расположение хранилища можно в [настройках модуля Кеер](#).
2. Если проблема с записью архива в локальное хранилище, то проверьте, что на жестких дисках достаточно свободного места для записи.
3. Если проблема с записью архива в сетевое хранилище, то проверьте его сетевую доступность аналогично тому, как [проверяется доступность камеры](#).
4. В настройках камеры проверьте, правильное ли указано хранилище и [включена ли запись архива](#).

Для обращения в техподдержку

Чтобы специалисты техподдержки скорее смогли решить вашу проблему, заранее соберите дампы сетевого трафика между ПО Insentry и IP-камерой в момент [ручного добавления камеры](#) и воспроизведения потоков (см. *Руководство пользователя*, раздел *Просмотр живого видео и архива*) и приложите файл дампа при создании обращения.

Контакты техподдержки:

Телефон: +7 (495) 540-47-44

Почта: support@insentry.io

Телеграм: [@insentry_support](https://t.me/insentry_support)

Видеопоток не воспроизводится

1. Проверьте, совпадают ли порты (HTTP, RTSP, ONVIF), [указанные в ПО Insentry](#), с теми, что указаны в веб-интерфейсе камеры.
2. Выполните диагностику работы видеопотока или обратитесь в техническую поддержку.

Для обращения в техподдержку

Чтобы специалисты техподдержки скорее смогли решить вашу проблему, заранее соберите дампы сетевого трафика между ПО Insentry и IP-камерой в момент [ручного добавления камеры](#) и воспроизведения потоков (см. *Руководство пользователя*, раздел *Просмотр живого видео и архива*) и приложите файл дампа при обращении в техподдержку.

Видеопоток работает нестабильно

При нестабильной работе видеопотока (картинка замирает, пропадает, рассыпается) в первую очередь необходимо проверить следующие условия:

- текущую пропускную способность канала связи с камерой;
- стабильность работы канала связи с камерой (интернет, VPN, локальная сеть).

Если с этими пунктами всё в порядке, то следует проверить работоспособность сервера, АРМ, камеры.

Проверка пропускной способности канала связи

Для стабильной передачи данных с камеры необходимо, чтобы пропускная способность канала была достаточной для передачи всего объёма данных.

Необходимые минимальные значения пропускной способности канала для стабильной работы одной камеры и ПО Insentry в зависимости от разрешения видеопотока:

Проверка текущей пропускной способности

Интернет-соединение

Скорость интернет-соединения можно проверить с помощью сайта <http://speedtest.net/ru>



VPN и локальная сеть

Проверку VPN или локальной сети необходимо проводить с помощью утилиты **iperf3**.

```

D:\iperf-3.1.3-win64>iperf3 -s
-----
Server listening on 5201
-----
Accepted connection from 127.0.0.1, port 52581
[ 5] local 127.0.0.1 port 5201 connected to 127.0.0.1 port 52582
[ ID] Interval      Transfer    Bandwidth
[ 5] 0.00-1.00 sec   317 MBytes  2.66 Gbits/sec
[ 5] 1.00-2.00 sec   322 MBytes  2.70 Gbits/sec
[ 5] 2.00-3.00 sec   322 MBytes  2.71 Gbits/sec
[ 5] 3.00-4.00 sec   348 MBytes  2.92 Gbits/sec
[ 5] 4.00-5.00 sec   352 MBytes  2.95 Gbits/sec
[ 5] 5.00-6.00 sec   358 MBytes  3.01 Gbits/sec
[ 5] 6.00-7.00 sec   361 MBytes  3.03 Gbits/sec
[ 5] 7.00-8.00 sec   362 MBytes  3.04 Gbits/sec
[ 5] 8.00-9.00 sec   361 MBytes  3.03 Gbits/sec
[ 5] 9.00-10.00 sec  359 MBytes  3.01 Gbits/sec
[ 5] 10.00-10.00 sec 933 KBytes  2.98 Gbits/sec
-----
[ ID] Interval      Transfer    Bandwidth
[ 5] 0.00-10.00 sec 0.00 Bytes  0.00 bits/sec
[ 5] 0.00-10.00 sec 3.38 GBytes 2.90 Gbits/sec
-----
Server listening on 5201
-----

```

Проверка стабильности работы канала связи

Вне зависимости от того, какой тип канала связи используется для взаимодействия между камерой и компьютером, на котором запущено ПО Insentry, для диагностики нужно определить доступность всех узлов и скорость их отклика.

Определение узлов на пути до камеры

Для определения списка узлов между локальным компьютером и камерой используйте команду `tracert` для Windows или `traceroute` для Linux. Желательно проверить все соединения: камера-сервер, сервер-APM, камера-APM.

- Для Windows:

Пуск > Выполнить > `cmd` > `tracert ip_адрес_назначения`.

Выбрать C:\Windows\system32\cmd.exe

```

Microsoft Windows [Version 10.0.14393]
(c) Корпорация Майкрософт (Microsoft Corporation), 2016. Все права защищены.

C:\Users\Anon>tracert 81.88.86.37

Трассировка маршрута к 81.88.86.37
с максимальным числом прыжков 30:

 1  <1 ms    <1 ms    <1 ms  KEENETIC_LTE [192.168.1.1]
 2  2 ms     1 ms     1 ms   broadband-90-154-77-162.ip.moscow.rt.ru [90.154.77.162]
 3  2 ms     1 ms     1 ms   77.37.250.202
 4  1 ms     1 ms     1 ms   msk-m9-rt08-gi-0-0-123.mangotele.com [195.208.209.97]
 5  2 ms     2 ms     2 ms   81.88.84.59
 6  2 ms     2 ms     2 ms   81.88.86.37

Трассировка завершена.
C:\Users\Anon>

```

- Для Linux:

Открыть терминал > `traceroute ip_адрес_назначения -n`

```

root@linux-pc1:~#
root@linux-pc1:~# traceroute 60.0.0.2 -n
traceroute to 60.0.0.2 (60.0.0.2), 30 hops max, 60 byte packets
 1  10.0.0.2  6.530 ms  16.533 ms  25.841 ms
 2  20.0.0.2  35.820 ms  45.823 ms  56.077 ms
 3  123.0.0.3  65.522 ms  75.493 ms  85.302 ms
 4  123.0.0.4  95.317 ms  105.760 ms  115.671 ms
 5  50.0.0.2  125.708 ms  135.663 ms  145.536 ms
 6  60.0.0.2  155.537 ms  159.479 ms  159.540 ms
root@linux-pc1:~#

```

Поиск неисправного узла

Неисправным узлом будем называть тот, который отвечает с задержкой, тем самым снижая скорость передачи данных с камеры, что и вызывает её нестабильную работу.

Чтобы найти неисправный узел, выполните команду `ping` и проверить отклик от каждого узла в трассировке. В зависимости от типа соединения (оптика, DSL, спутник) отклик может быть разным. Также обязательно задать размер отправляемого пакета **1472** байта для проверки прохождения корректных значений **MTU**.

- Для Windows:

Пуск > выполнить > cmd > `ping -f -l 1472 ip_адрес_назначения`

```

Администратор: Командная строка
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corporation), 2009. Все права защищены.

C:\Users\Roman>ping -t vk.com

Обмен пакетами с vk.com [95.213.11.149] с 32 байтами данных:
Ответ от 95.213.11.149: число байт=32 время=2мс TTL=60
Ответ от 95.213.11.149: число байт=32 время=2мс TTL=60
Ответ от 95.213.11.149: число байт=32 время=1мс TTL=60
Ответ от 95.213.11.149: число байт=32 время=1мс TTL=60
Ответ от 95.213.11.149: число байт=32 время=1мс TTL=60

Статистика Ping для 95.213.11.149:
    Пакетов: отправлено = 5, получено = 5, потеряно = 0
    (0% потеря)
    Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 2 мсек, Среднее = 1 мсек
Control-C
^C
C:\Users\Roman>_
  
```

- Для Linux:

Открыть терминал > `ping -s 1472 ip_адрес_назначения`

```

[admin@server321 ~]$ ping -s 1472 172.17.13.20
PING 172.17.13.20 (172.17.13.20) 1472(1500) bytes of data.
1480 bytes from 172.17.13.20: icmp_seq=1 ttl=128 time=0.283 ms
1480 bytes from 172.17.13.20: icmp_seq=2 ttl=128 time=0.181 ms
1480 bytes from 172.17.13.20: icmp_seq=3 ttl=128 time=0.182 ms
1480 bytes from 172.17.13.20: icmp_seq=4 ttl=128 time=0.478 ms
1480 bytes from 172.17.13.20: icmp_seq=5 ttl=128 time=0.255 ms
1480 bytes from 172.17.13.20: icmp_seq=6 ttl=128 time=0.217 ms
1480 bytes from 172.17.13.20: icmp_seq=7 ttl=128 time=0.234 ms
1480 bytes from 172.17.13.20: icmp_seq=8 ttl=128 time=0.314 ms
1480 bytes from 172.17.13.20: icmp_seq=9 ttl=128 time=0.701 ms
1480 bytes from 172.17.13.20: icmp_seq=10 ttl=128 time=0.171 ms
1480 bytes from 172.17.13.20: icmp_seq=11 ttl=128 time=15.7 ms
1480 bytes from 172.17.13.20: icmp_seq=12 ttl=128 time=0.403 ms
1480 bytes from 172.17.13.20: icmp_seq=13 ttl=128 time=0.144 ms
^C
--- 172.17.13.20 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 83ms
rtt min/avg/max/mdev = 0.144/1.480/15.688/4.104 ms
[admin@server321 ~]$
  
```

Для обращения в техподдержку

Чтобы специалисты техподдержки скорее смогли решить вашу проблему, заранее соберите дампы сетевого трафика между ПО Insentry и IP-камерой в момент [ручного добавления камеры](#) и воспроизведения потоков (см. *Руководство пользователя*, раздел *Просмотр живого видео и архива*) и приложите файл дампа при создании обращения.

Контакты техподдержки:

Телефон: [+7 \(495\) 540-47-44](tel:+74955404744)

Почта: support@insentry.io

Телеграм: [@insentry_support](https://t.me/insentry_support)

Insentry.Keep не видит сетевое хранилище или не хватает прав для его использования

Модуль Insentry.Keep работает от встроенной учетной записи *Система* (System), а не от учетной записи пользователя. Поэтому если вы добавили диск на свою учетную запись, то Keep может не хватать прав на использование хранилища.

В этом случае попытке добавить сетевое хранилище возникает ошибка `Folder doesn't exist and cannot be created` и сетевой диск не появляется при выборе в меню добавления хранилища.

Для того чтобы разрешить учетной записи *Система* использовать хранилище:

1. Скачайте утилиту [Sysinternals Suite](#) и распакуйте архив в любую удобную папку (для примера назовём её `C:\sysinternals`)
2. Откройте командную строку с правами администратора и перейдите в каталог утилиты:
`cd C:\sysinternals`
3. Выполните команду `psexec -i -s cmd.exe` . Откроется новая консоль с супер-правами пользователя Система.
4. В этой консоли выполните команду для добавления сетевого хранилища, вместо диска z используйте букву уже добавленного хранилища на вашей учетной записи: `net use {z}: \\{servername}\\{sharedfolder} /persistent:yes`
5. Для удаления хранилища выполните команду `net use {z}: /delete`
Не выполняйте этот шаг, если не хотите удалить хранилище
6. Закройте консоли, перейдите в корневой каталог диска `C:\`
7. Создайте файл **disk.txt** и откройте его с помощью блокнота.
8. В файл добавьте следующую строку: `net use {z}: \\{servername}\\{sharedfolder} /persistent:yes`
9. Не меняя каталога, сохраните текстовый файл как **disk.bat**.
10. В планировщике заданий Windows нажмите кнопку **Создать задачу**.
11. В поле **Имя** напишите **mapping**.
12. Нажмите кнопку **Изменить** при выборе учетной записи
13. Введите **СИСТЕМА** в верхнем регистре и нажмите кнопку **Проверить имена**. Если при этом не удастся найти учётную запись, нажмите **Дополнительно → Поиск → Выбрать запись → СИСТЕМА**.
14. Во вкладке **Триггеры** нажмите кнопку **Создать** и выберите значение **Начать задачу при запуске**
15. Во вкладке **Действия** нажмите кнопку **Создать** и укажите путь до файла **disk.bat**.
16. Нажмите **ОК** и сохраните созданную задачу

Готово! Теперь сетевое хранилище будет автоматически добавляться пользователю *Система* при перезагрузке сервера.

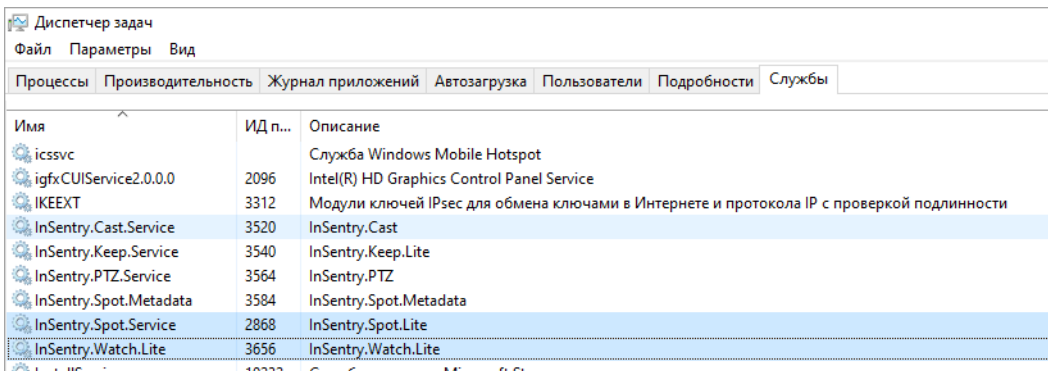
Не включается детектор (ползунок нельзя переключить)

Проблема связана с проверкой минимальных системных требований ПК, на котором установлено ПО InSentry.

Для включения некоторых детекторов (распознавание лиц, гос. номеров и т.д.) необходимо наличие графического процессора (видеокарты), соответствующего определённым требованиям. При запуске детектора InSentry проверяет видеокарту на соответствие этим требованиям, и блокирует возможность запустить детектор, если требования не выполняются.

Чтобы запустить детектор в тестовых целях, даже если видеокарта не соответствует минимальным требованиям, отключите проверку:

1. Остановите службы **Watch** и **Spot.Service**.



Имя	ИД п...	Описание
icssvc		Служба Windows Mobile Hotspot
igfxCUIService2.0.0.0	2096	Intel(R) HD Graphics Control Panel Service
IKEEXT	3312	Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности
InSentry.Cast.Service	3520	InSentry.Cast
InSentry.Keep.Service	3540	InSentry.Keep.Lite
InSentry.PTZ.Service	3564	InSentry.PTZ
InSentry.Spot.Metadata	3584	InSentry.Spot.Metadata
InSentry.Spot.Service	2868	InSentry.Spot.Lite
InSentry.Watch.Lite	3656	InSentry.Watch.Lite
InstallService	10222	Служба установки Microsoft Store

2. Откройте файл `application.properties` с помощью текстового редактора.

Расположение файла:

- Linux: `/usr/src/InSentry/Spot.Lite/application.properties`
- Windows: `C:\Program Files\InSentry\Spot.Lite\application.properties`

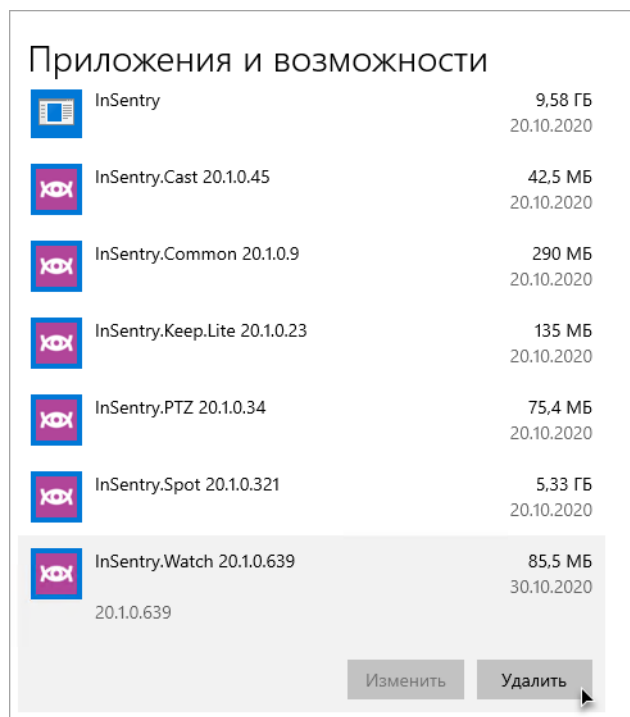
1. Измените параметр `syscheck.enabled=true` на `syscheck.enabled=false`.
2. Сохраните файл.
3. Включите службы **Watch** и **Spot.Service** через диспетчер задач.

Эта настройка предназначена только для тестирования работы детекторов и их настройки! Не выключайте проверку на постоянно работающих серверах — это может вызвать перегрузку и отказ системы.

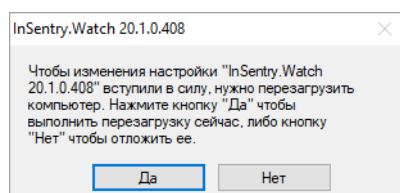
Не запускается клиент InSentry после переустановки модуля InSentry Watch

При удалении модуля InSentry Watch и его переустановки без перезагрузки, полностью пропадает доступ к InSentry. Чтобы восстановить доступ:

1. Удалите InSentry Watch стандартными средствами операционной системы (установка/удаление программ).



2. После удаления модуля перезагрузите компьютер.



3. Установите новую версию модуля.

4. После установки новой версии перезагрузите компьютер ещё раз.

Чтобы такая проблема не возникала, после удаления InSentry Watch всегда перезагружайте компьютер, прежде чем устанавливать новую версию модуля.

Восстановление базы данных из резервной копии

После внезапного отключения электричества может потребоваться восстановление базы данных из резервной копии.

База данных watch.db.mv.db находится в папке модуля Watch. Путь к папке модуля Watch при установке ПО InSentry по умолчанию:

- в Windows — **C:\ProgramData\InSentry\Watch.Lite**
- в Linux — **/var/lib/docker/volumes/insentry-data/_data/InSentry/Watch.Lite**

Резервные копии базы данных автоматически сохраняются в папке backup, расположенной там же.

Чтобы восстановить базу данных из резервной копии:

1. Остановите контейнер с InSentry Watch в Linux или службу InSentry.Watch.Lite в Windows.
2. В папке модуля Watch переименуйте файл watch.db.mv.db. Этот файл — старая база данных. Выберите для него любое имя.

3. Перенесите самый свежий файл резервной копии из папки backup в папку модуля — туда, где лежит база данных.
4. Переименуйте файл резервной копии в watch.db.mv.db.
5. Запустите контейнер с Insentry Watch или службу InSentry.Watch.Lite.

См. также: [Бэкап базы данных, лицензий и настроек](#)

Insentry.Cloud

Insentry.Cloud — облачная версия видеонаблюдения Insentry, которая позволяет смотреть видео с камер онлайн, записывать и хранить архив в облаке Insentry.

[Посмотреть тарифы на сайте →](#)

Начало работы в Insentry.Cloud

Регистрация

Чтобы начать работу с облаком Insentry, зарегистрируйтесь на портале [insentry.video](#).

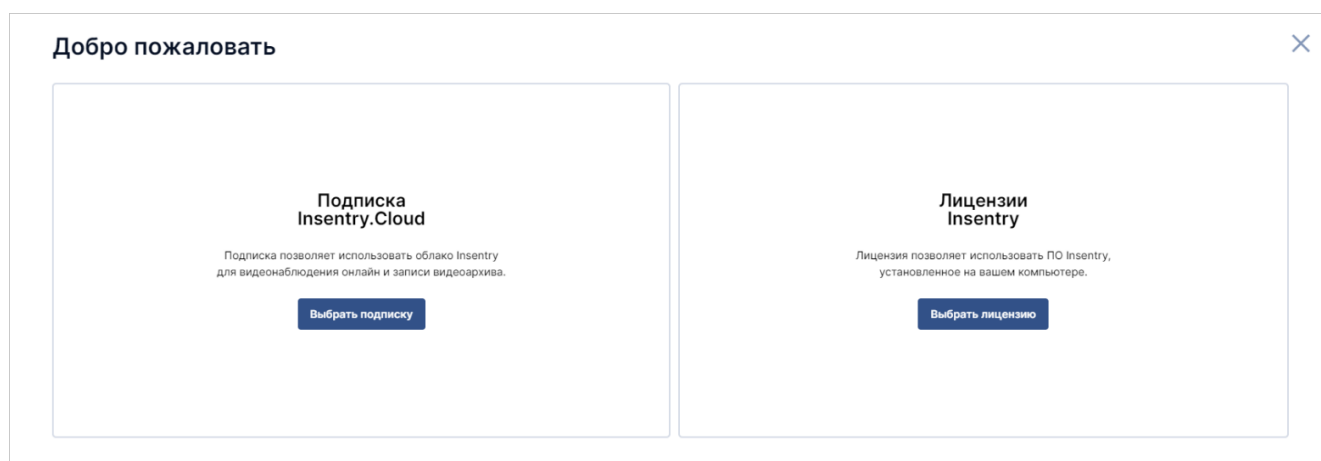
В качестве логина используйте электронную почту. Укажите действующий адрес почты, к которой у вас есть доступ.

После завершения регистрации вы сможете продолжить работу с облаком Insentry на портале [insentry.video](#):

1. оформить подписку;
2. подключить камеры.

Стартовый экран

После завершения регистрации вы увидите стартовый экран:



Подписка Insentry.Cloud позволяет использовать облако Insentry.Cloud. Облако Insentry.Cloud работает только по подписке, лицензия для него не требуется.

Лицензии Insentry позволяют подключать камеры к обычной, не облачной, версии Insentry, запущенной на вашем сервере или компьютере.

Вы можете использовать облачную и серверную версии Insentry одновременно. Для этого нужно будет оформить и подписку, и лицензию.

Купить или изменить тариф подписки, выбрать или сменить лицензию можно в любой момент в личном кабинете на портале insentry.video.

Подписка

Для оформления подписки на стартовом экране нажмите кнопку **Выбрать подписку** и выберите один из вариантов подписки. В бесплатном тарифе доступно только видеонаблюдение. Архив и другие функции доступны в платных тарифных планах.

[Подробнее описание тарифов на сайте →](#)

Посмотреть информацию о выбранной подписке и перечень доступных услуг, а также сменить тариф можно в разделе **Личный кабинет → Моя подписка**.

Для начала работы с Insentry, [подключите камеры к облаку](#).

Подключение камер к Insentry.Cloud

Подключить камеры к облаку Insentry.Cloud можно несколькими способами:

1. [через роутер](#);
2. [через обычный или одноплатный компьютер](#);
3. [с помощью серверной версии Insentry.Watch](#);
4. [с помощью Insentry.Bridge](#);
5. [напрямую через интернет](#).

Рекомендации по выбору способа подключения:

1. Подключение через роутер или компьютер требует настройки проброса портов.
2. Подключение с помощью серверной версии Insentry.Watch позволяет смотреть через облачную версию видео с камер, подключенных к серверной версии. Сложных настроек в этом случае не потребуется. Вы можете хранить в облаке архив камер, подключенных к серверной версии, если оформите одну из платных подписок.
3. Подключить камеры к облаку через Insentry.Bridge — самый простой способ. В этом случае не потребуется никаких дополнительных настроек.
4. Подключить напрямую через интернет можно только камеры со статическим публичным IP. Этот вариант не является рекомендованным, потому что без VPN доступ к данным ваших камер могут получить третьи лица.

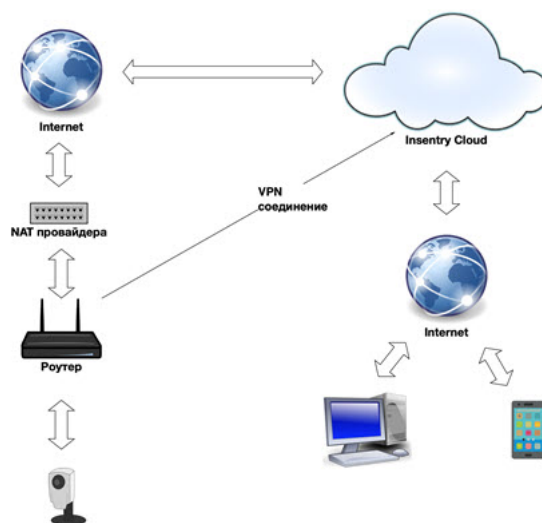
Способ подключения	Достоинства	Недостатки
Подключение через роутер	Роутер обычно уже есть дома, а если нет, то его несложно купить	Требуется настройка VPN и проброса портов
Подключение через обычный компьютер	Не нужно покупать роутер	Требуется настройка VPN и проброса портов

Способ подключения	Достоинства	Недостатки
Подключение через одноплатный компьютер	Одноплатный компьютер стоит намного дешевле обычного	Сложная настройка, требуется знание ОС Linux
Подключение с помощью серверной версии Insentry.Watch	Простая настройка	Требуется установить Insentry на ваш компьютер
Подключение с помощью Insentry.Bridge	Простая настройка	Требуется приобрести Insentry.Bridge
Подключение напрямую через интернет	Простая настройка	Доступ к данным ваших камер не защищён; публичный IP — платный

Подключение камер к Insentry.Cloud через роутер

Для подключения камер к облаку Insentry.Cloud могут быть использованы бытовые роутеры, имеющие встроенный OpenVPN-клиент.

Схема подключения:



Такая схема подключения полностью работоспособна в сетях провайдеров, использующих NAT: так как никаких входящих соединений со стороны Internet роутер не принимает, для реализации схемы не требуется получать у провайдера ни статический, ни динамический белый IP.

Подключение через роутер Keenetic (Zyxel)

- [Получение файла VPN-конфигурации](#)
- [Установка OpenVPN](#)
- [Настройка OpenVPN](#)
- [Проброс портов](#)
- [Подключение камер](#)

Получение файла VPN-конфигурации

1. Перейдите в раздел **Управление → Система → VPN-Соединения**.
2. Укажите логин VPN-соединения — для каждого компьютера должен использоваться отдельный логин.

Если скачать ключи повторно с тем логином, который уже используется, сертификат будет обновлён, а соединение будет разорвано. Для продолжения работы нужно будет заново настроить соединение.

3. Нажмите кнопку **Скачать**.

The screenshot shows the 'VPN-соединения' (VPN connections) section of the system settings. On the left, there is a table listing existing connections. On the right, there is a 'Настройка VPN-соединения' (VPN connection settings) section with instructions and a download button.

Логин	Время подключения	Активно	
17985E0AC4E6	23.12.2024, 23:10:46	Да	Удалить
raf	-	Нет	Удалить
home_VPN	26.08.2024, 11:37:04	Нет	Удалить
client157	23.12.2024, 23:13:23	Да	Удалить
client	12.09.2024, 22:40:39	Нет	Удалить

Настройка VPN-соединения

Инструкции по подключению камер к Insentry.Cloud:

- через роутер Keenetic
- через роутер Mikrotik
- через обычный или одноплатный компьютер

1. Скачайте архив с ключами и файлом конфигурации

[Скачать](#)
Повторное скачивание ключей аннулирует ранее созданные ключи
2. Настройте OpenVPN-клиент на роутере или компьютере на подключение к серверу Insentry Cloud

Адрес: insentry.video
 Порт: 1194
 Протокол: TCP
 Логин: client
 Пароль: client
3. Настройте на роутере или компьютере проброс портов камер через VPN-соединение

Для каждой камеры нужно пробросить HTTP и RTSP-порты.
 Требуемый диапазон портов: 10000-10999
4. Нажмите кнопку «Автообнаружение» на [Странице добавления камер](#) и добавьте камеры в систему

4. Сохраните и распакуйте zip-архив с ключами и файлом конфигурации.

Установка OpenVPN

Поддержка VPN-клиента и сервера OpenVPN реализована во всех современных роутерах Keenetic, работающих на базе операционной системы KeeneticOS версии 3.1.x и старше. OpenVPN устанавливается через программный компонент системы. После установки роутер может работать как OpenVPN-клиент или OpenVPN-сервер (режим определяется конфигурацией, заданной в файле *.ovpn).

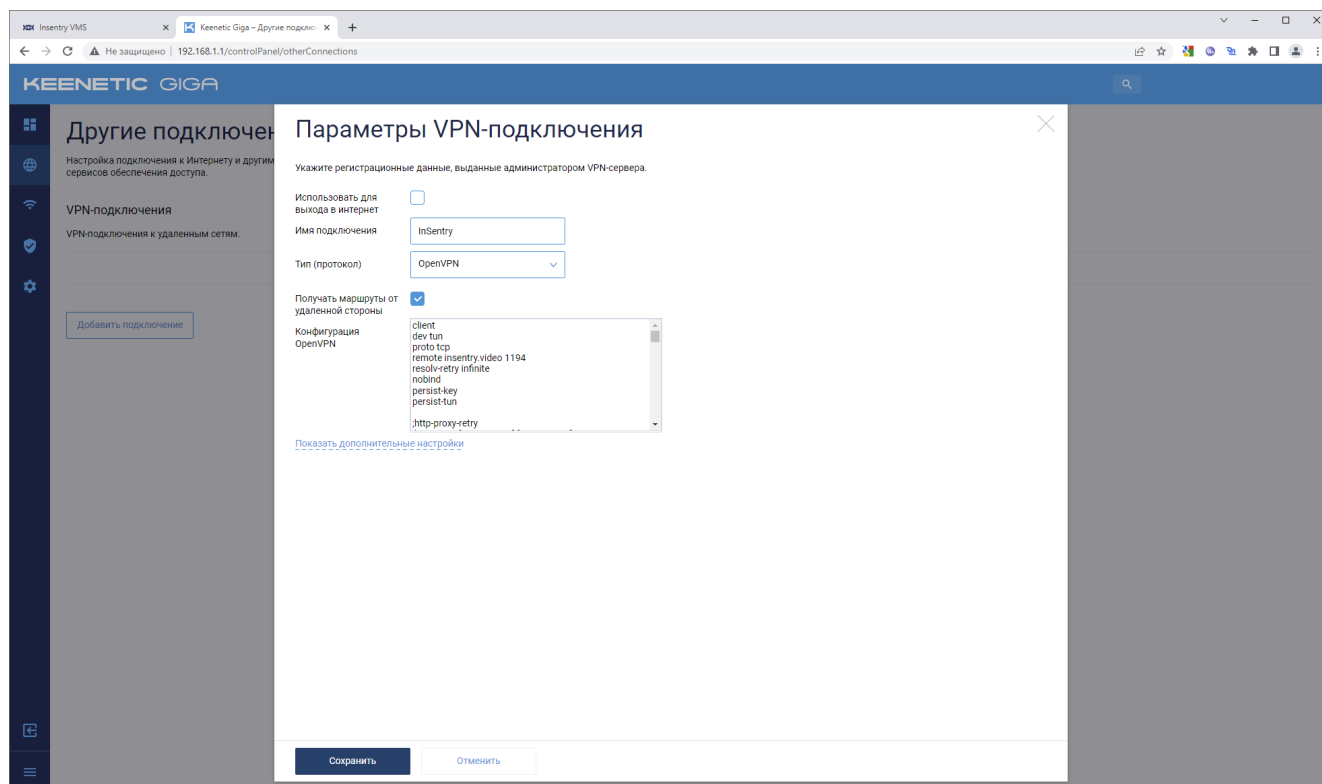
Для установки OpenVPN:

1. В настройках роутера откройте раздел **Общие настройки системы**.
2. Нажмите кнопку **Изменить набор компонентов**.
3. В поисковой строке начните вводить «Openvpn». В списке найденных компонентов проявится **Клиент и сервер OpenVPN**.
4. Если компонент не установлен, установите его. При установке будет выбрана самая свежая версия компонента.

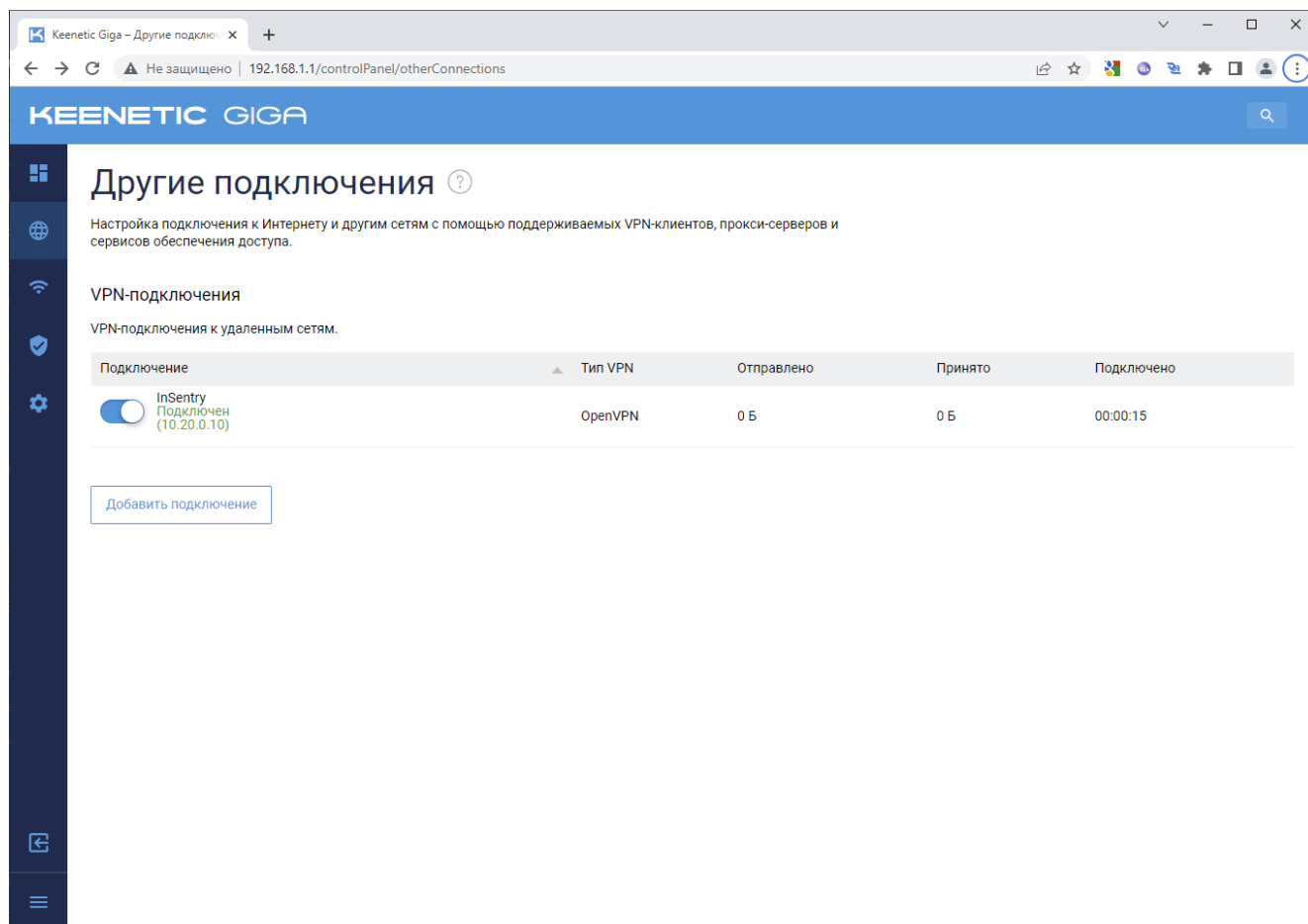
См. также: [Клиент и сервер OpenVPN](#)

Настройка OpenVPN

1. В настройках роутера откройте раздел **Другие подключения**.
2. Создайте новое VPN-подключение со следующими параметрами:
 - **Имя подключения:** InSentry
 - **Протокол:** OpenVPN
 - **Получать маршруты:** Да
3. Скопируйте содержимое файла insentry.ovpn из загруженного архива в поле **Конфигурация OpenVPN**.



4. Нажмите кнопку **Сохранить** и включите VPN-соединение:



Когда соединение будет установлено, на странице настроек VPN-соединения в интерфейсе InSentry.Cloud отобразится информация о нём.

Проброс портов

Роутер является VPN-клиентом InSentry.Cloud, но непосредственного доступа в его локальную сеть у служб InSentry.Cloud нет: им доступны только порты самого роутера в его VPN-соединении. Для того, чтобы у InSentry.Cloud появился доступ к камерам, находящимся в локальной сети роутера, нужно настроить переадресацию HTTP и RTSP портов роутера на соответствующие порты камер.

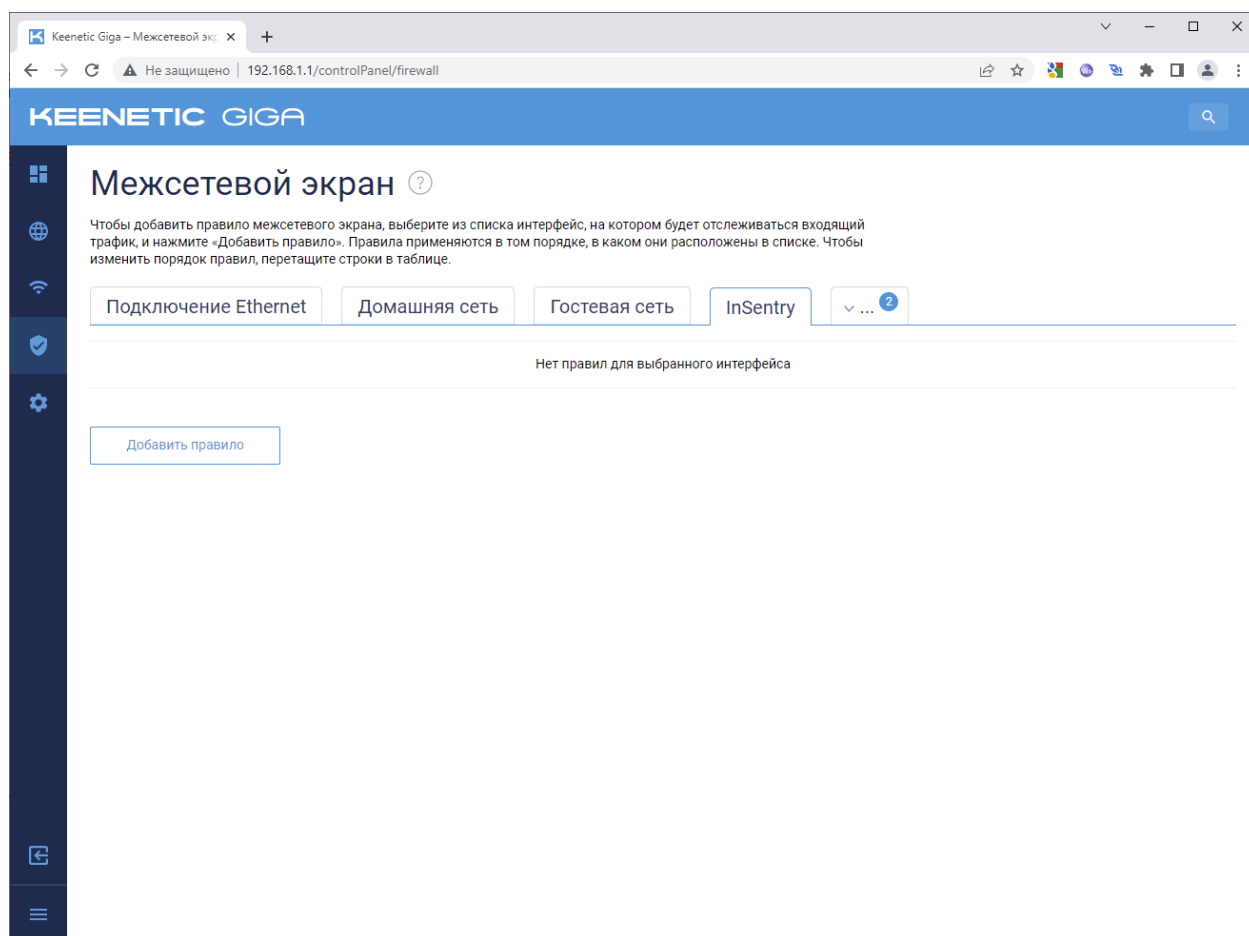
Составьте список IP-адресов камер, подключенных через роутер, которые необходимо подключить к InSentry.

У каждой камеры есть два TCP-порта: 80 (протокол HTTP) и 554 (протокол RTSP). Необходимо настроить на роутере переадресацию портов так, чтобы соединения на TCP-порты из диапазона 10000-10999, открытые в VPN-соединении с InSentry.Cloud, попадали на 80 и 554 TCP-порты камер.

В процессе настройки переадресации придерживайтесь следующих правил:

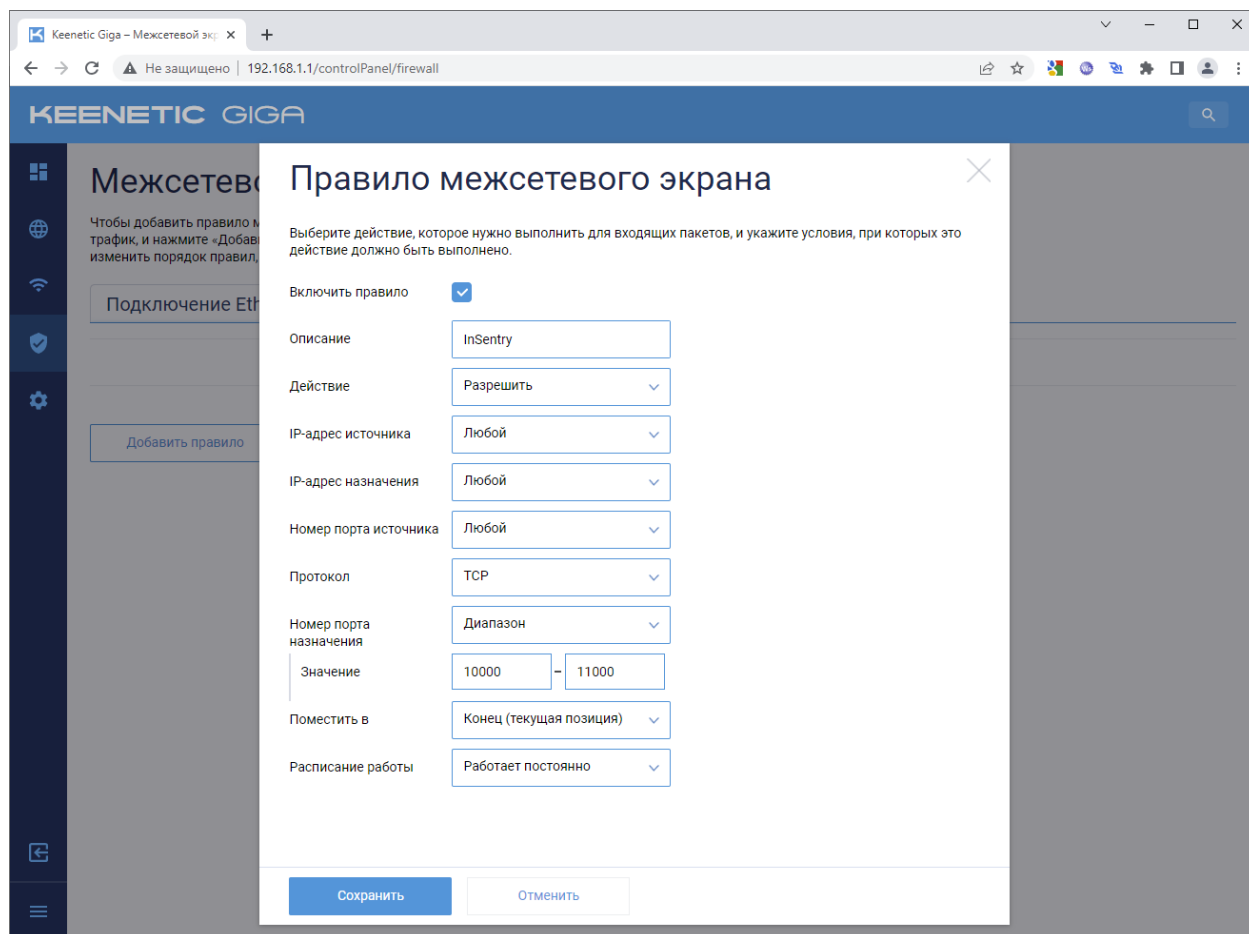
- соединения с чётных портов из диапазона 10000-10998 необходимо перенаправлять на 80 порты камер (например, порт 10000 из VPN-соединения на 80 порт камеры);
- соединения со следующего по порядку нечетного порта необходимо перенаправлять на 554 порт той же камеры (например, порт 10001 из VPN-соединения на 554 порт камеры);
- для одного VPN соединения сброшенные порты на камеры не должны пересекаться — для каждой камеры должен быть свой индивидуальный порт.

1. В настройках роутера откройте вкладку **Межсетевой экран** и выберите соединение InSentry:

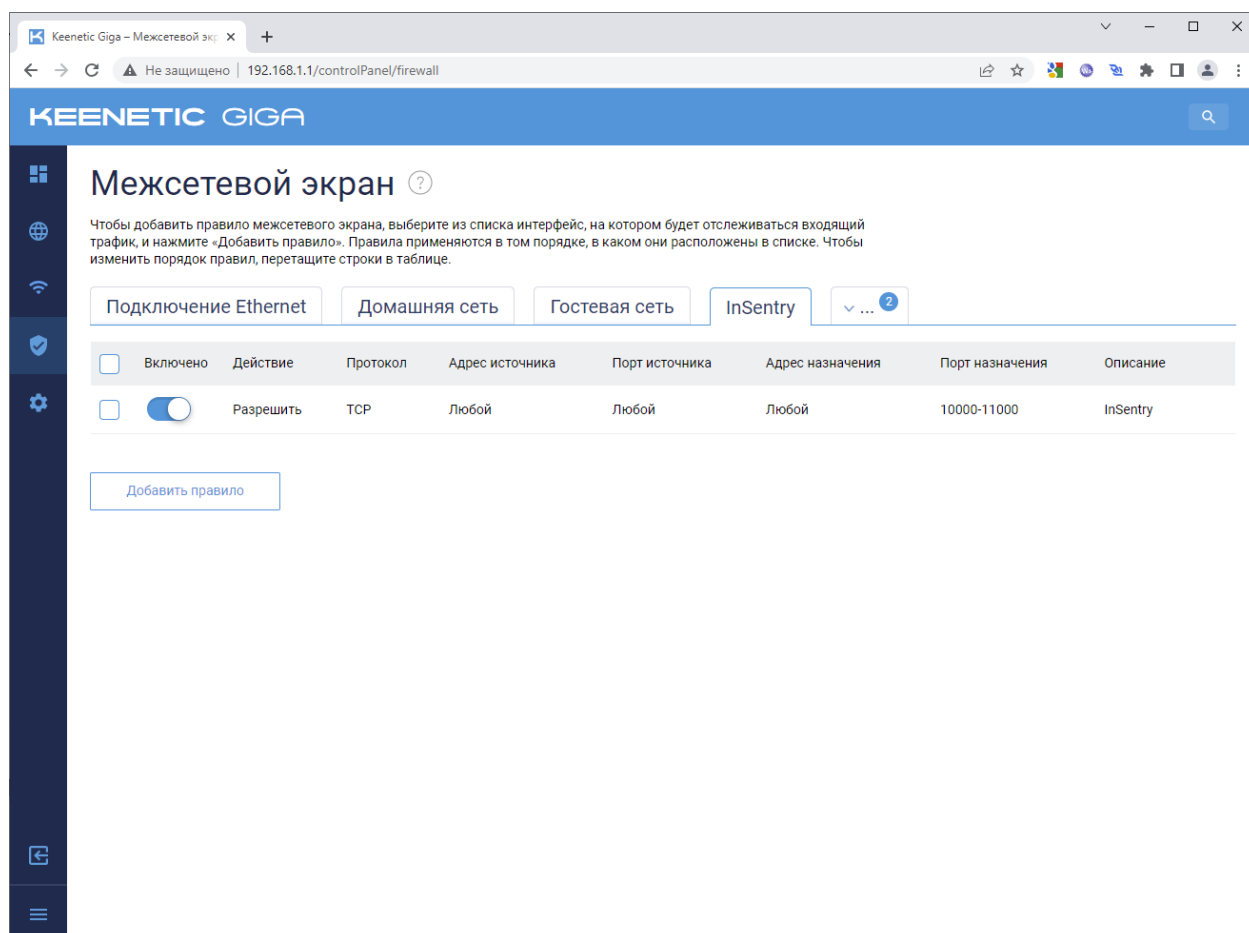


2. Нажмите кнопку **Добавить правило** и заполните параметры:

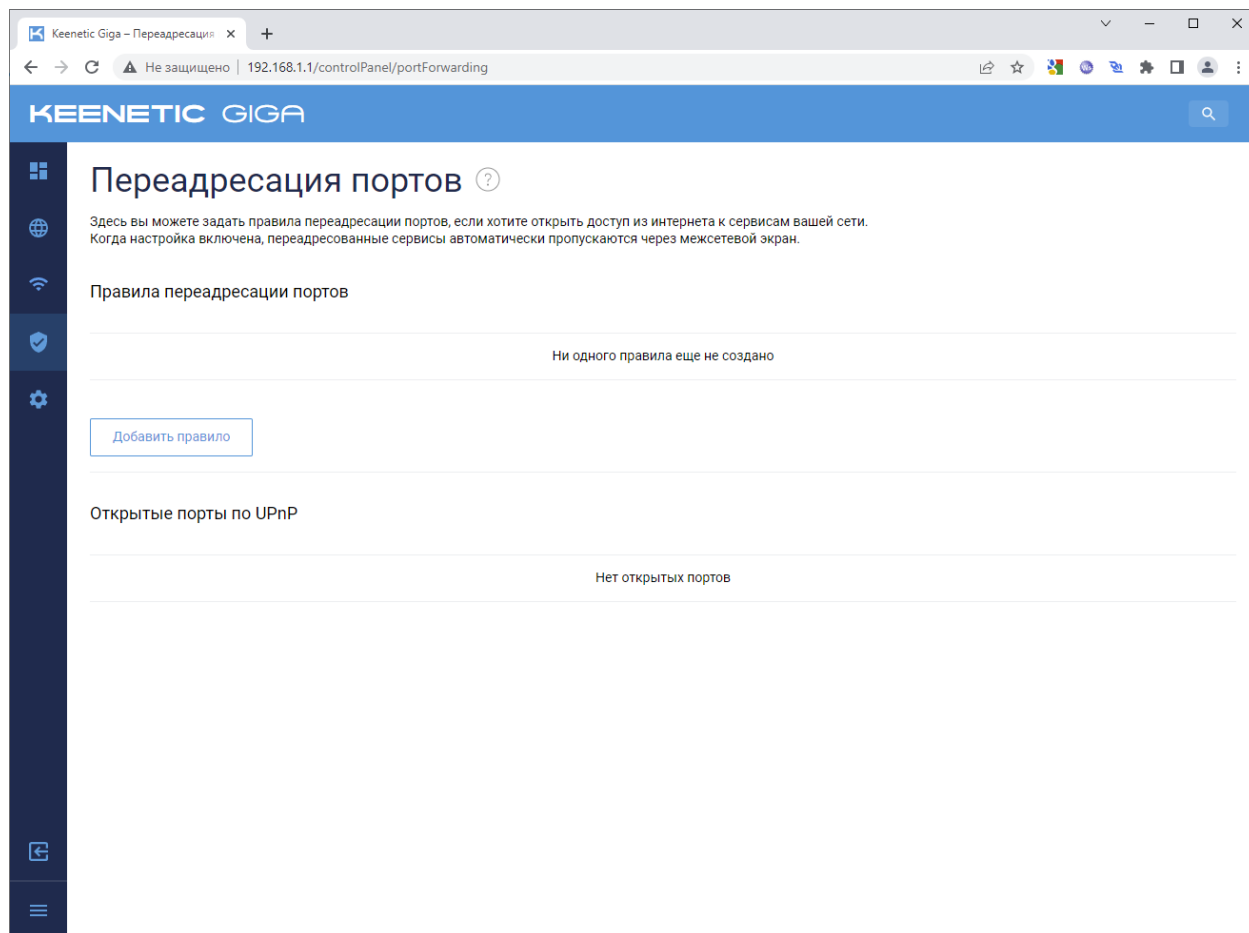
- **Включить правило:** Да
- **Действие:** Разрешить
- **IP-адрес источника:** Любой
- **IP-адрес назначения:** Любой
- **Протокол:** TCP
- **Номер порта назначения:** Диапазон
- **Значение:** 10000 – 10999
- **Поместить в:** Конец
- **Расписание работы:** Работает постоянно



3. Нажмите кнопку **Сохранить**. Проверьте, что всё настроено верно:

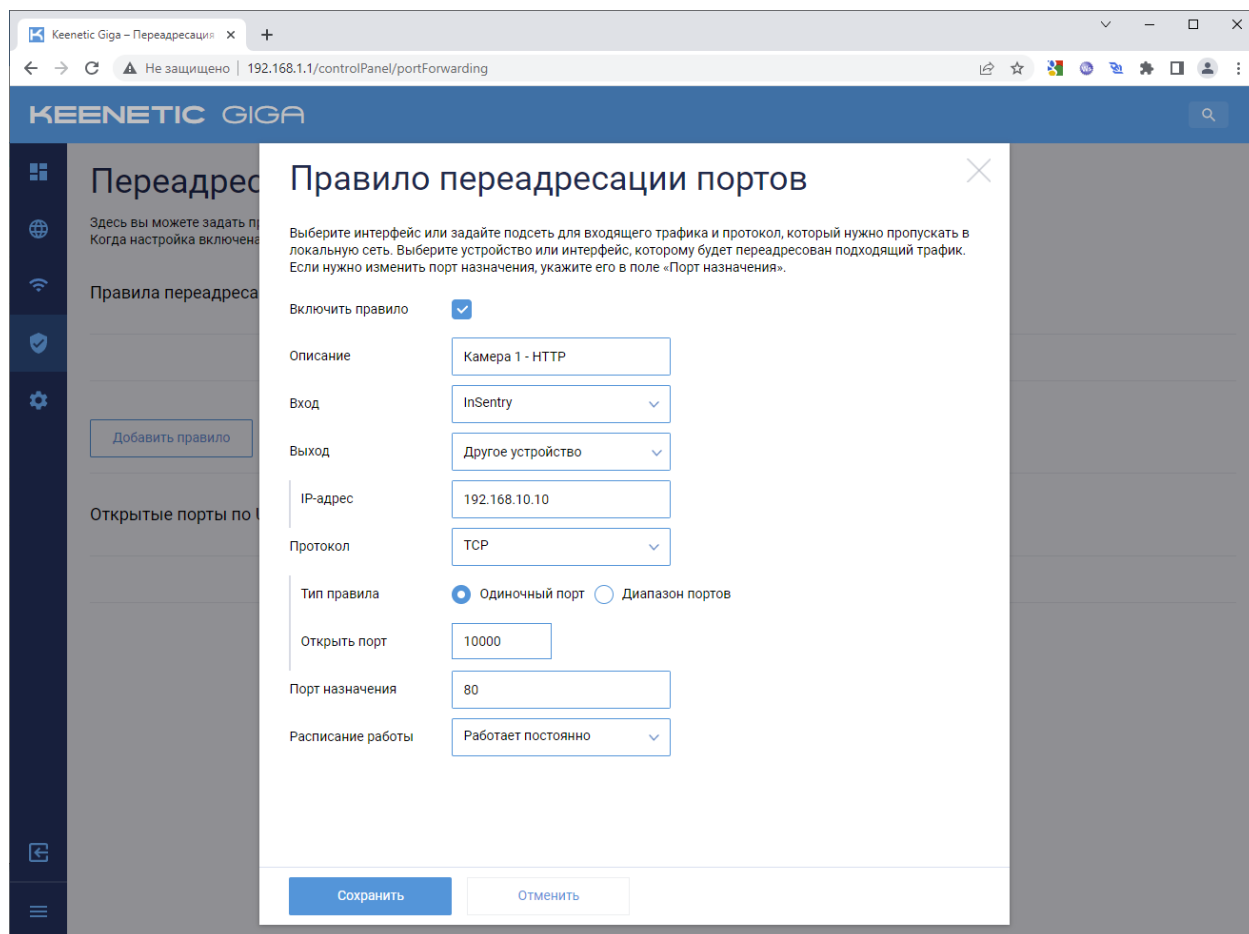


4. Перейдите на страницу **Переадресация портов**.



5. Нажмите кнопку **Добавить правило** и укажите параметры нового правила:

- **Включить правило:** Да
- **Описание:** Название камеры и название протокола: HTTP
- **Вход:** InSentry (название VPN-соединения)
- **Выход:** Другое устройство
- **IP-адрес:** IP-адрес камеры
- **Протокол:** TCP
- **Тип правила:** Одиночный порт
- **Открыть порт:** Чётный номер порта из диапазона 10000-10998 (не занятый другими камерами)
- **Порт назначения:** 80
- **Расписание работы:** Работает постоянно



6. Нажмите кнопку **Сохранить**, после чего аналогичным образом настройте переадресацию RTSP-порта той же камеры:
- **Включить правило:** Да
 - **Описание:** Название камеры и название протокола: RTSP
 - **Вход:** InSentry (название VPN-соединения)
 - **Выход:** Другое устройство
 - **IP-адрес:** IP-адрес камеры
 - **Протокол:** TCP
 - **Тип правила:** Одиночный порт
 - **Открыть порт:** Нечётный номер порта из диапазона 10000-10999, который на единицу больше, чем номер, введенный для протокола HTTP
 - **Порт назначения:** 554
 - **Расписание работы:** Работает постоянно

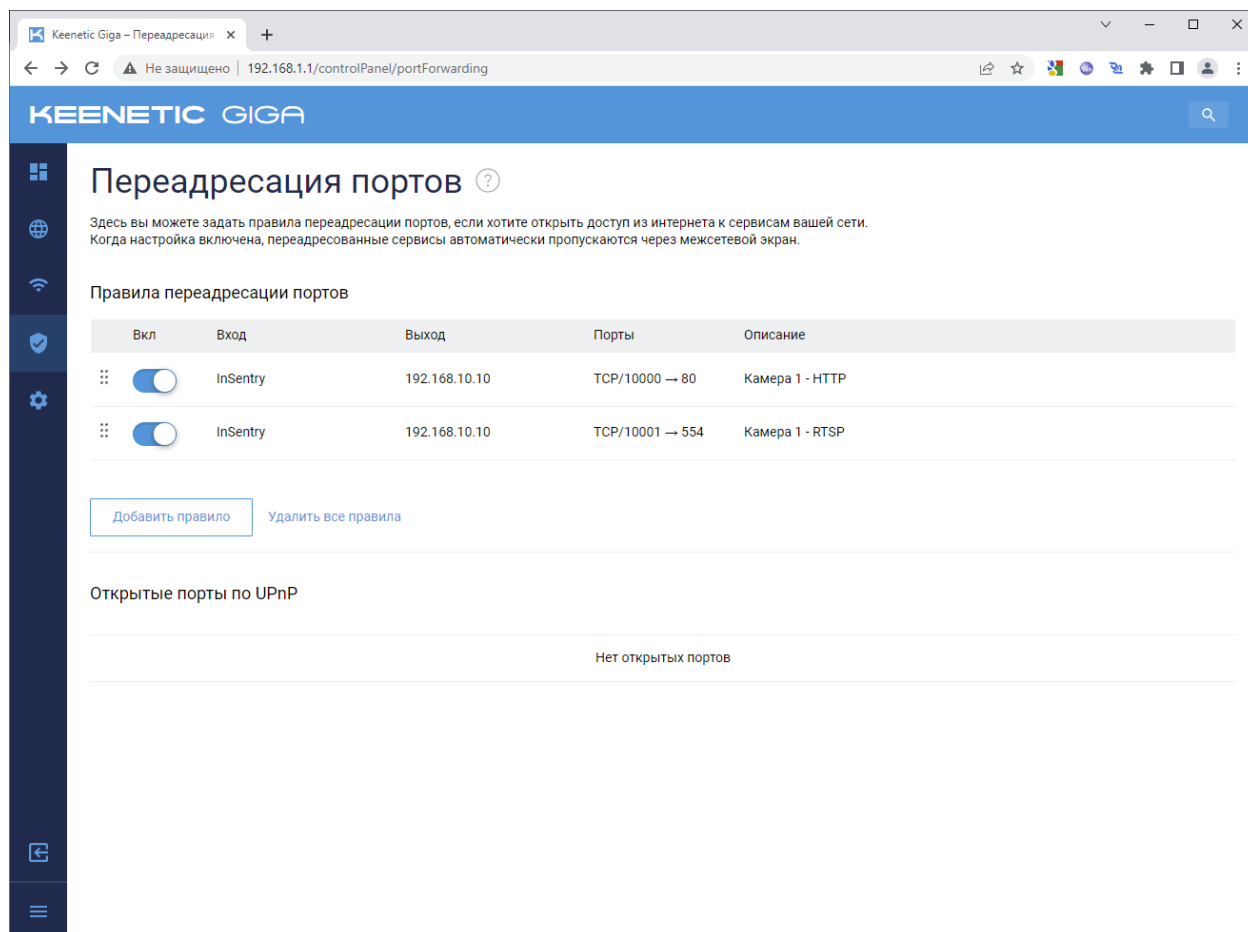
The screenshot shows the Keenetic Giga web interface in a browser. The address bar shows the URL `192.168.1.1/controlPanel/portForwarding`. The main heading is "Правило переадресации портов" (Port Forwarding Rule). Below the heading, there is a description: "Выберите интерфейс или задайте подсеть для входящего трафика и протокол, который нужно пропускать в локальную сеть. Выберите устройство или интерфейс, которому будет переадресован подходящий трафик. Если нужно изменить порт назначения, укажите его в поле «Порт назначения»." (Select an interface or specify a subnet for incoming traffic and the protocol that needs to be passed to the local network. Select a device or interface to which the appropriate traffic will be forwarded. If you need to change the destination port, specify it in the "Destination port" field.).

The configuration fields are as follows:

- Включить правило (Enable rule): ☒
- Описание (Description): Камера 1 - HTTP
- Вход (Source): InSentry
- Выход (Destination): Другое устройство
- IP-адрес (IP address): 192.168.10.10
- Протокол (Protocol): TCP
- Тип правила (Rule type): ☒ Одиночный порт (Single port), ☐ Диапазон портов (Port range)
- Открыть порт (Open port): 10001
- Порт назначения (Destination port): 554
- Расписание работы (Schedule): Работает постоянно

At the bottom, there are two buttons: "Сохранить" (Save) and "Отменить" (Cancel).

7. Нажмите **Сохранить**. В результате настройки переадресация портов камеры должна выглядеть следующим образом:



Если камер несколько, необходимо пробросить их порты аналогичным образом, используя другие номера портов из диапазона от 10000 до 10999.

См. также: [Инструкция по пробросу портов на сайте keenetic.com](https://keenetic.com/ru/help/10000-10999/)

Добавление камер из локальной сети через VPN

После того, как предыдущие шаги были завершены, OpenVPN-соединение с роутером активно и порты камер были успешно переадресованы в настройках роутера, можно приступать к подключению камер к облаку Insentry.

1. Откройте клиент Insentry на портале insentry.video.
2. В разделе **Управление → Устройства → Камеры → Мастер добавления**.
3. Укажите логин и пароль для доступа к камере.
4. Запустите проверку соединения.
5. Выберите одну или несколько из обнаруженных камер, успешно прошедших проверку, и нажмите **Добавить выбранные**.
6. Следуя шагам мастера добавления, завершите процесс.

После этого камеры будут подключены к облачной версии Insentry и доступны для просмотра на портале insentry.video.

Подключение через роутер MikroTik

- [Получение файла VPN-конфигурации](#)
- [Настройка OpenVPN](#)
- [Проброс портов](#)
- [Подключение камер](#)

Получение файла VPN-конфигурации

1. Перейдите в раздел **Управление → Система → VPN-Соединения**.
2. Укажите логин VPN-соединения — для каждого компьютера должен использоваться отдельный логин.

Если скачать ключи повторно с тем логином, который уже используется, сертификат будет обновлён, а соединение будет разорвано. Для продолжения работы нужно будет заново настроить соединение.

3. Нажмите кнопку **Скачать**.

Система > VPN-соединения

VPN-соединения

Логин	Время подключения	Активно	
17985E0AC4E6	23.12.2024, 23:10:46	Да	Удалить
raf	-	Нет	Удалить
home_VPN	26.08.2024, 11:37:04	Нет	Удалить
client157	23.12.2024, 23:13:23	Да	Удалить
client	12.09.2024, 22:40:39	Нет	Удалить

Настройка VPN-соединения

Инструкции по подключению камер к Insentry.Cloud:

- через роутер Keenetic
- через роутер MikroTik
- через обычный или одноплатный компьютер

1. Скачайте архив с ключами и файлом конфигурации

[Скачать](#)
Повторное скачивание ключей аннулирует ранее созданные ключи
2. Настройте OpenVPN-клиент на роутере или компьютере на подключение к серверу Insentry Cloud

Адрес: insentry.video
Порт: 1194
Протокол: TCP
Логин: client
Пароль: client

Если вам необходимо подключить несколько роутеров, используйте для них разные логины (латинские буквы, минимум 6 символов)
3. Настройте на роутере или компьютере проброс портов камер через VPN-соединение

Для каждой камеры нужно пробросить HTTP и RTSP-порты.

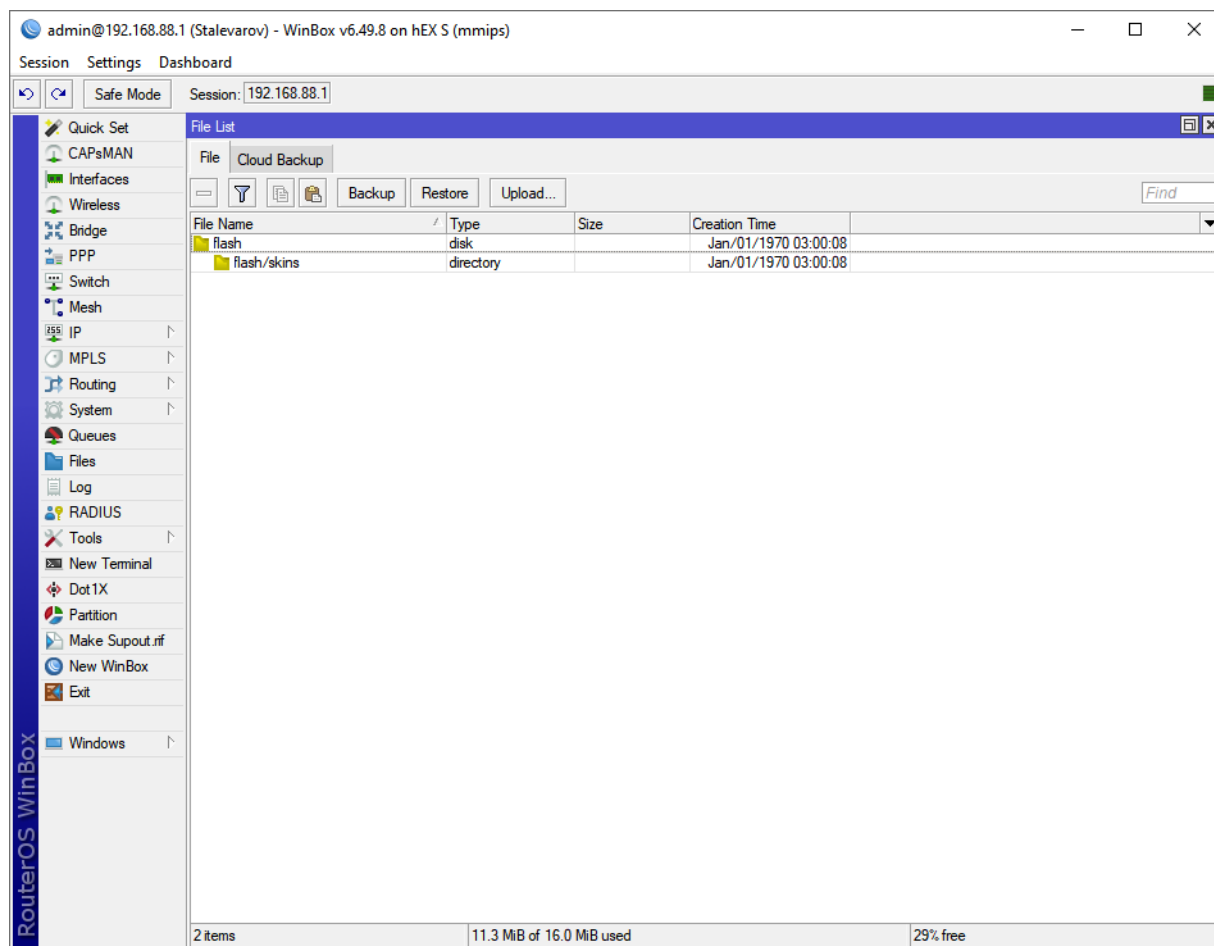
Номер RTSP-порта камеры при пробросе должен быть на единицу больше, чем ее номер HTTP-порта

Требуемый диапазон портов:
10000-10999
4. Нажмите кнопку «Автообнаружение» на [Странице добавления камер](#) и добавьте камеры в систему

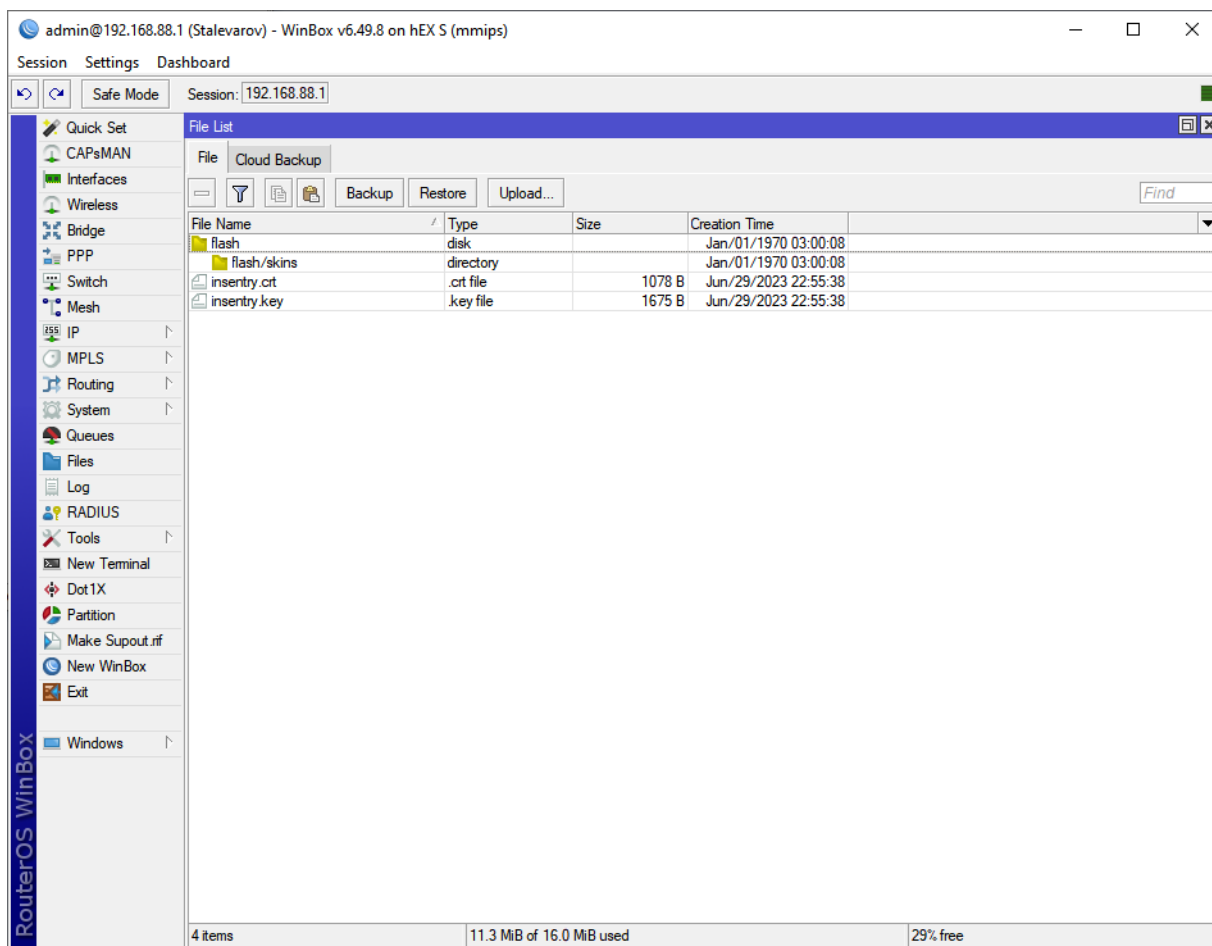
4. Сохраните и распакуйте zip-архив с ключами и файлом конфигурации.

Настройка OpenVPN

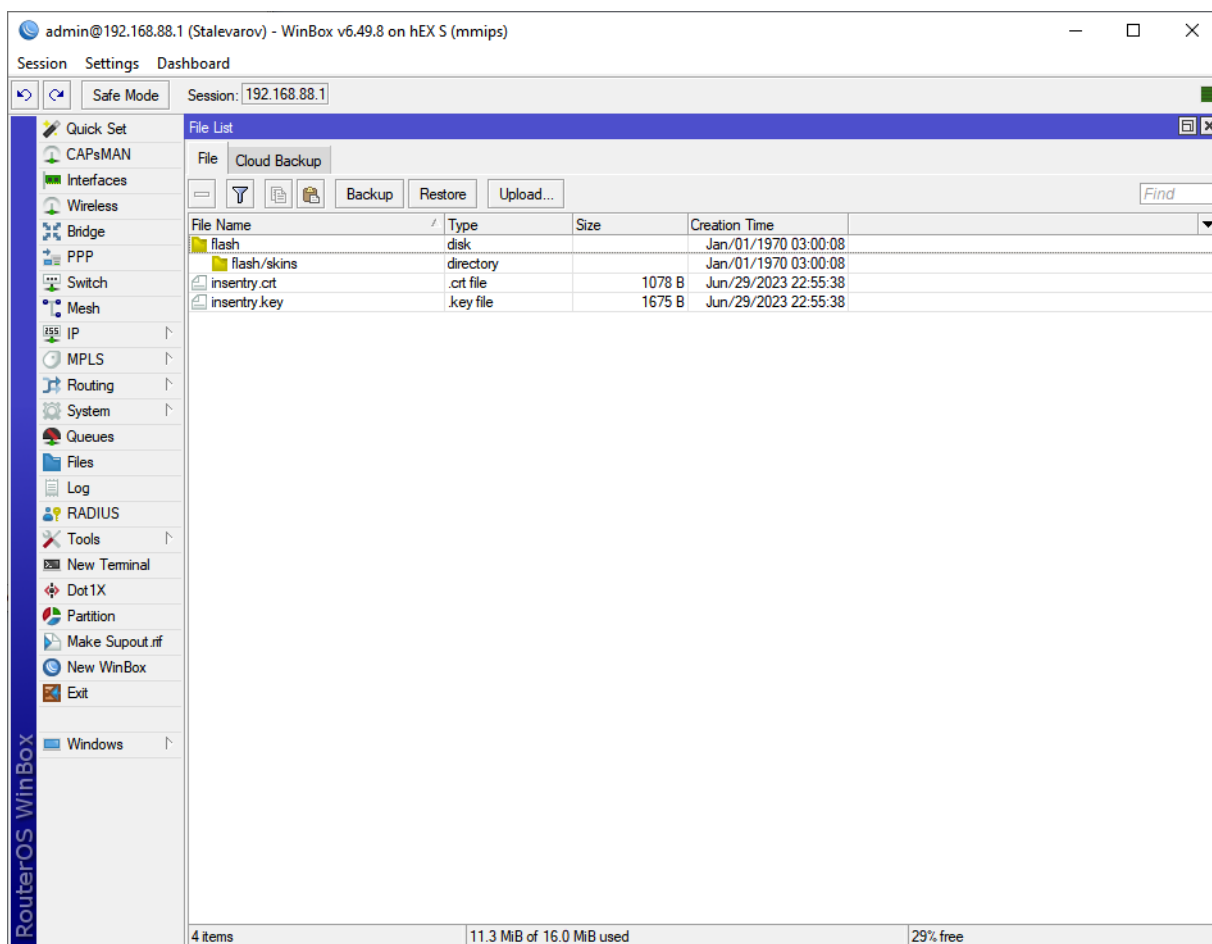
1. Откройте WinBox.
2. Перейдите в меню Files:



3. Нажмите кнопку **Upload** и выберите файлы **insentry.crt** и **insentry.key** из скачанного ранее архива с ключами. Загруженные файлы будут отображены в окне:



4. Перейдите в раздел **System → Certificates**:

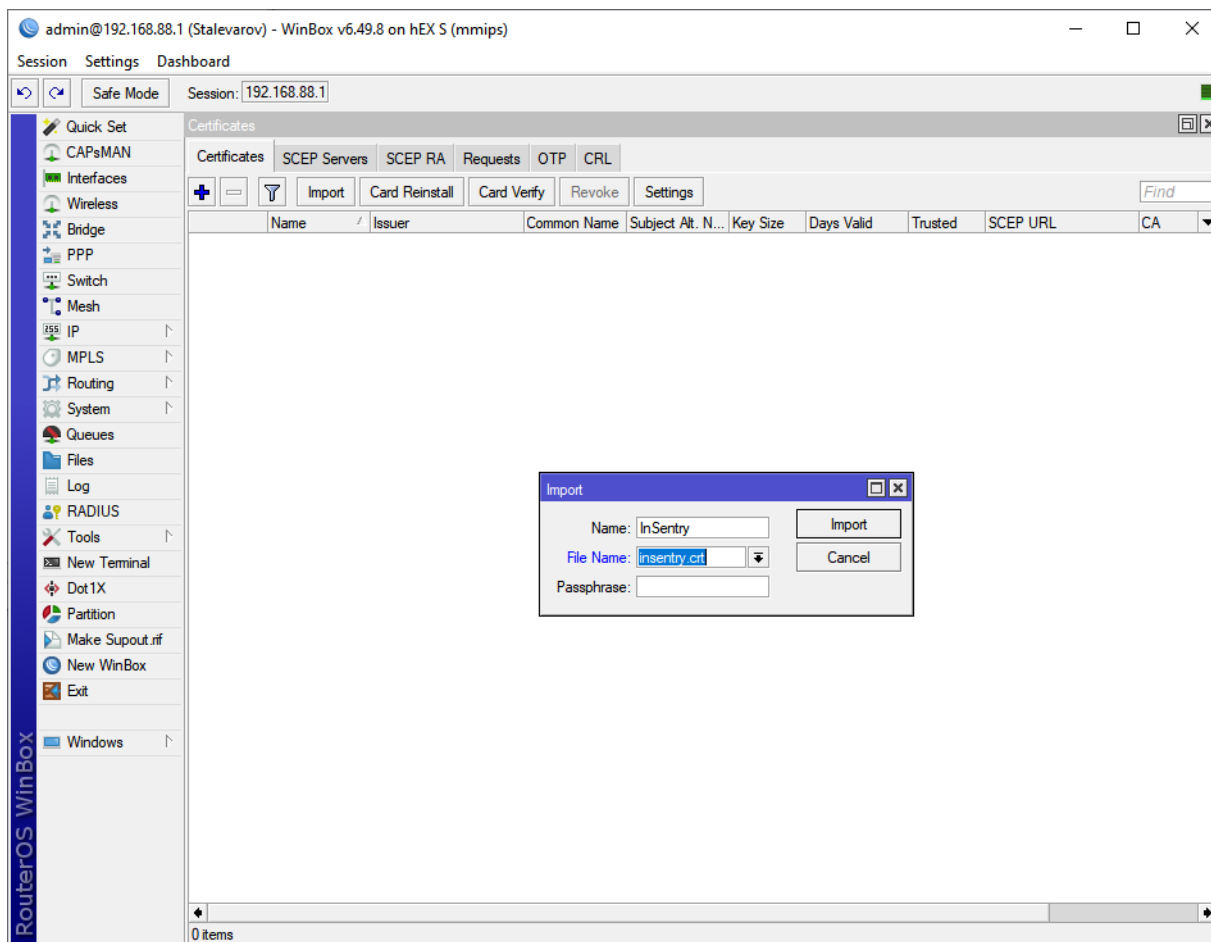


5. Нажмите кнопку **Import**. В открывшемся окне заполните поля:

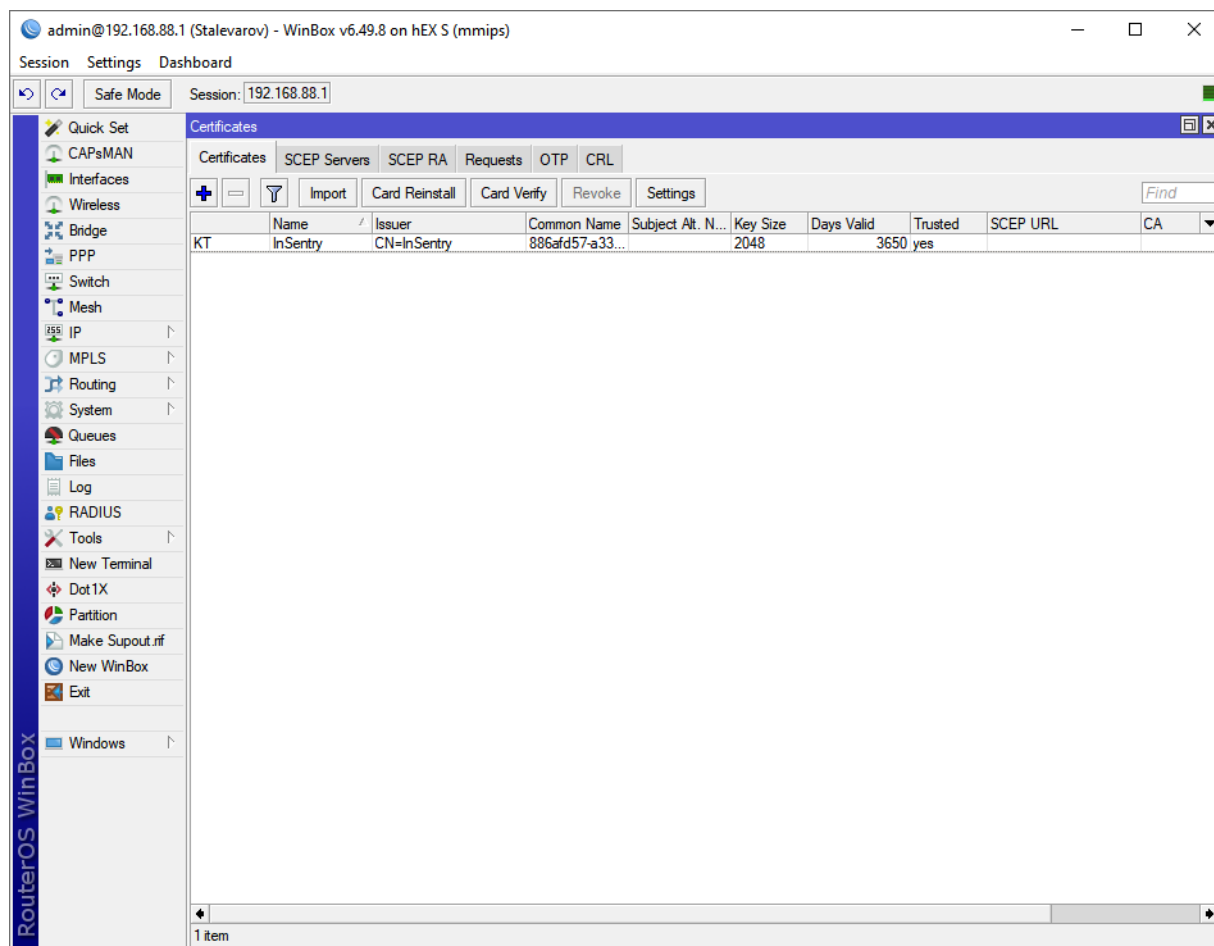
- **Name:** InSentry
- **File Name:** insentry.crt
- **Passphrase:** оставьте пустым

6. Нажмите кнопку **Import**. Начнётся импорт сертификата.

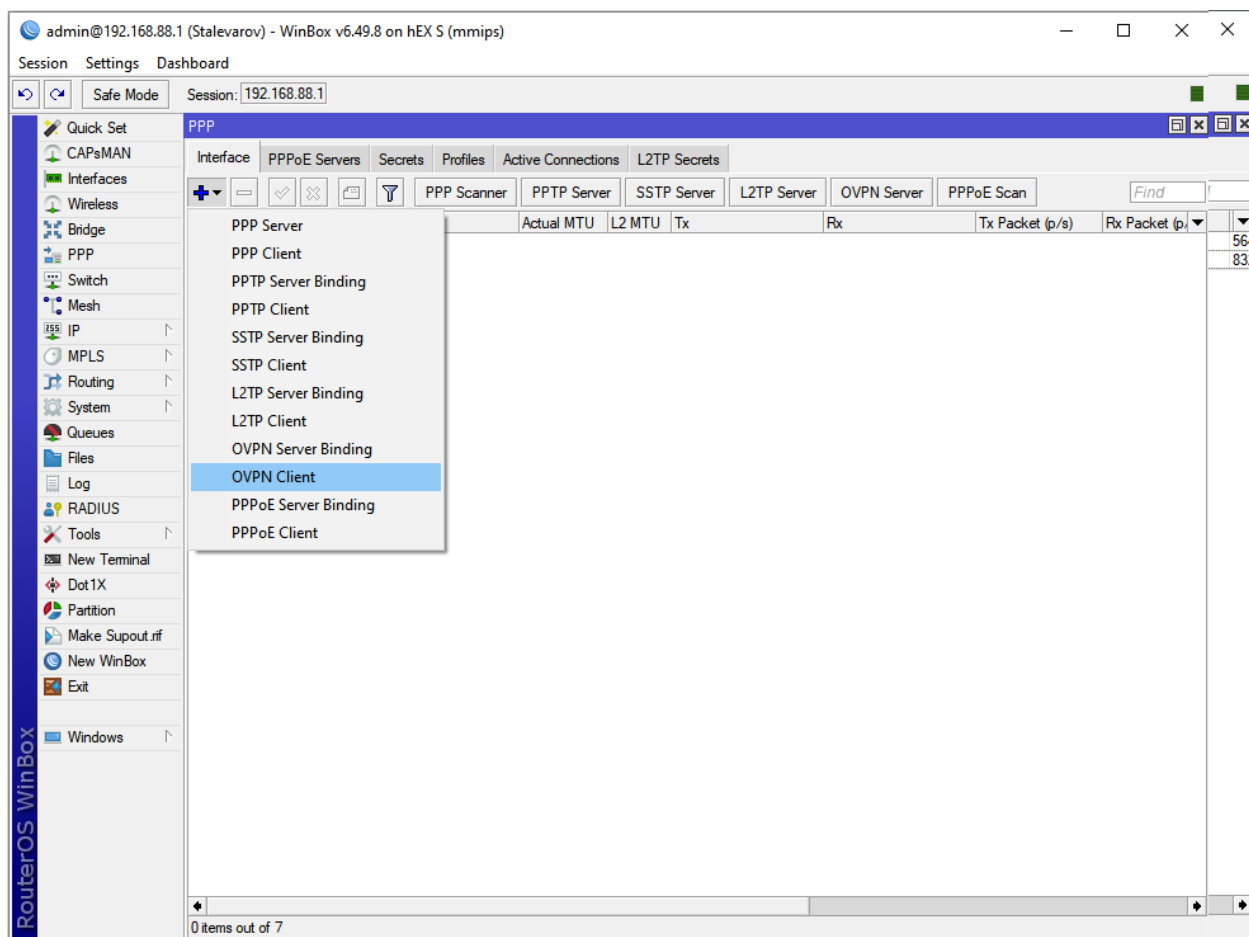
7. Повторите эти действия для импорта ключа, выбрав в поле **File Name** файл *insentry.key*.



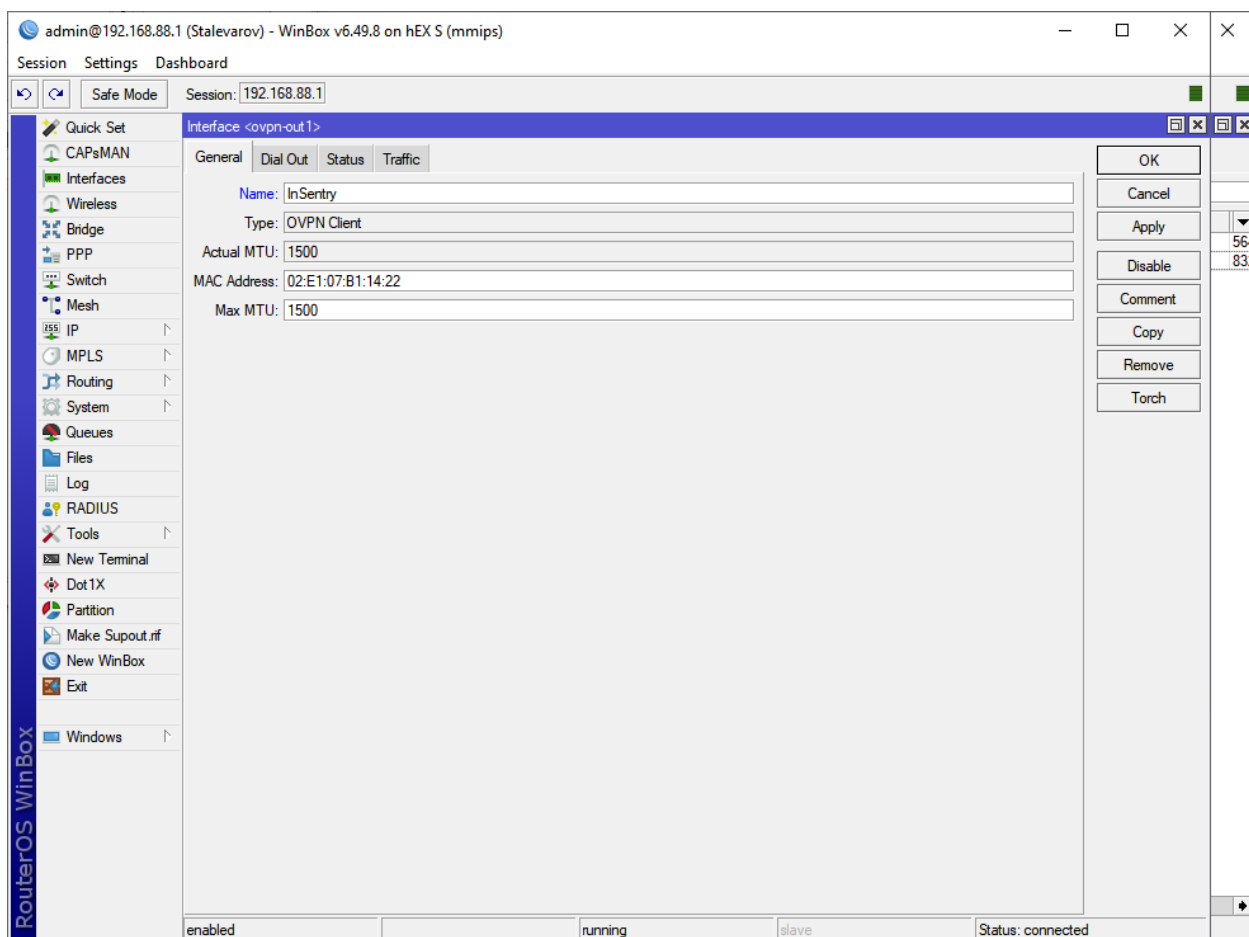
В результате должен появиться сертификат, в первом столбце которого выводятся буквы **КТ** (это означает, что есть сертификат и ключ к нему).



8. Перейдите в раздел **PPP** на вкладку **Interface**. Нажмите на плюс «+» и выберите **OVPN Client**:



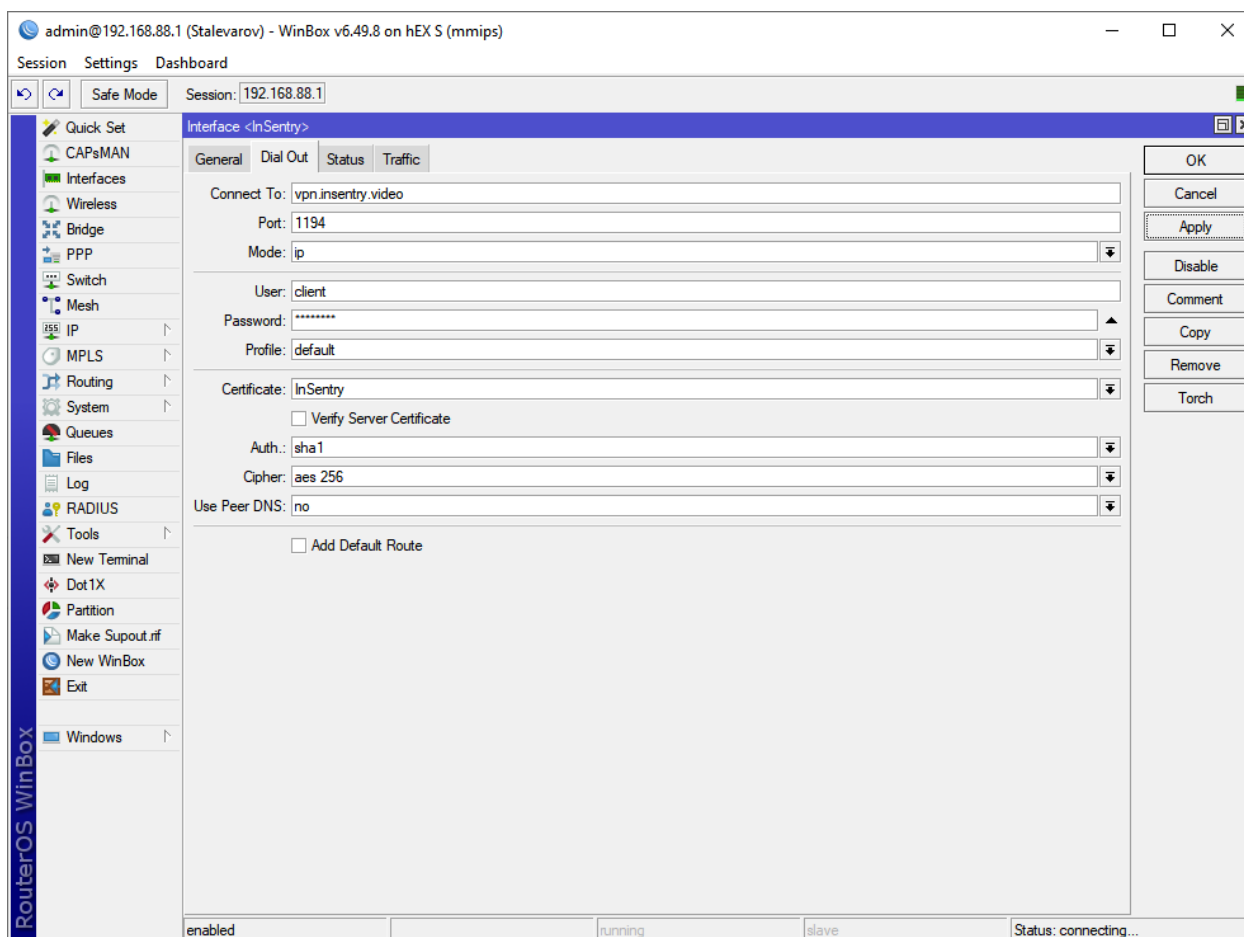
9. В открывшемся окне на вкладке **General** в поле **Name** укажите InSentry:



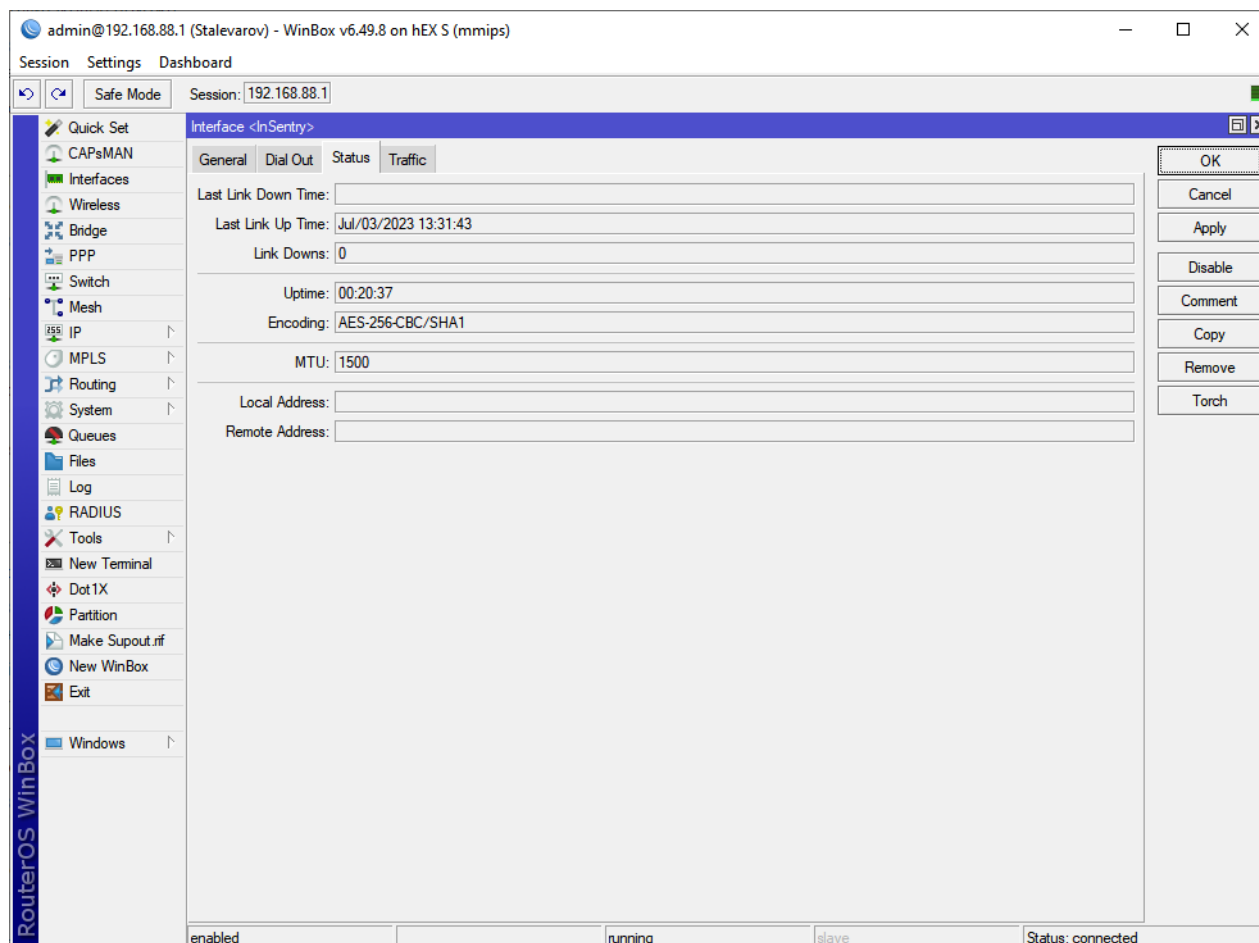
10. Перейдите на вкладку **Dial Out** и заполните поля:

- **Connect To:** vpn.insentry.video
- **Port:** 1194
- **Mode:** IP
- **Protocol:** TCP (поле присутствует только на роутерах MikroTik начиная с RouterOS 7. Если этого поля нет, значит, TCP используется по умолчанию)
- **User:** client
- **Password:** insentry
- **Profile:** default
- **Certificate:** InSentry
- **Verify Server Certificate:** нет (оставьте пустым)
- **Auth:** sha1
- **Cipher:** aes 256
- **Use peer DNS:** no

11. Заполнив поля, нажмите кнопку **OK**:



Если соединение успешно установилось, вкладка **Status** будет выглядеть так:



Когда соединение будет установлено, на странице настроек VPN-соединения в интерфейсе InSentry.Cloud отобразится информация о нём.

Проброс портов

Роутер является VPN-клиентом InSentry.Cloud, но непосредственного доступа в его локальную сеть у служб InSentry.Cloud нет: им доступны только порты самого роутера в его VPN-соединении. Для того, чтобы у InSentry.Cloud появился доступ к камерам, находящимся в локальной сети роутера, нужно настроить переадресацию HTTP и RTSP портов роутера на соответствующие порты камер.

Составьте список IP-адресов камер, подключенных через роутер, которые необходимо подключить к InSentry.

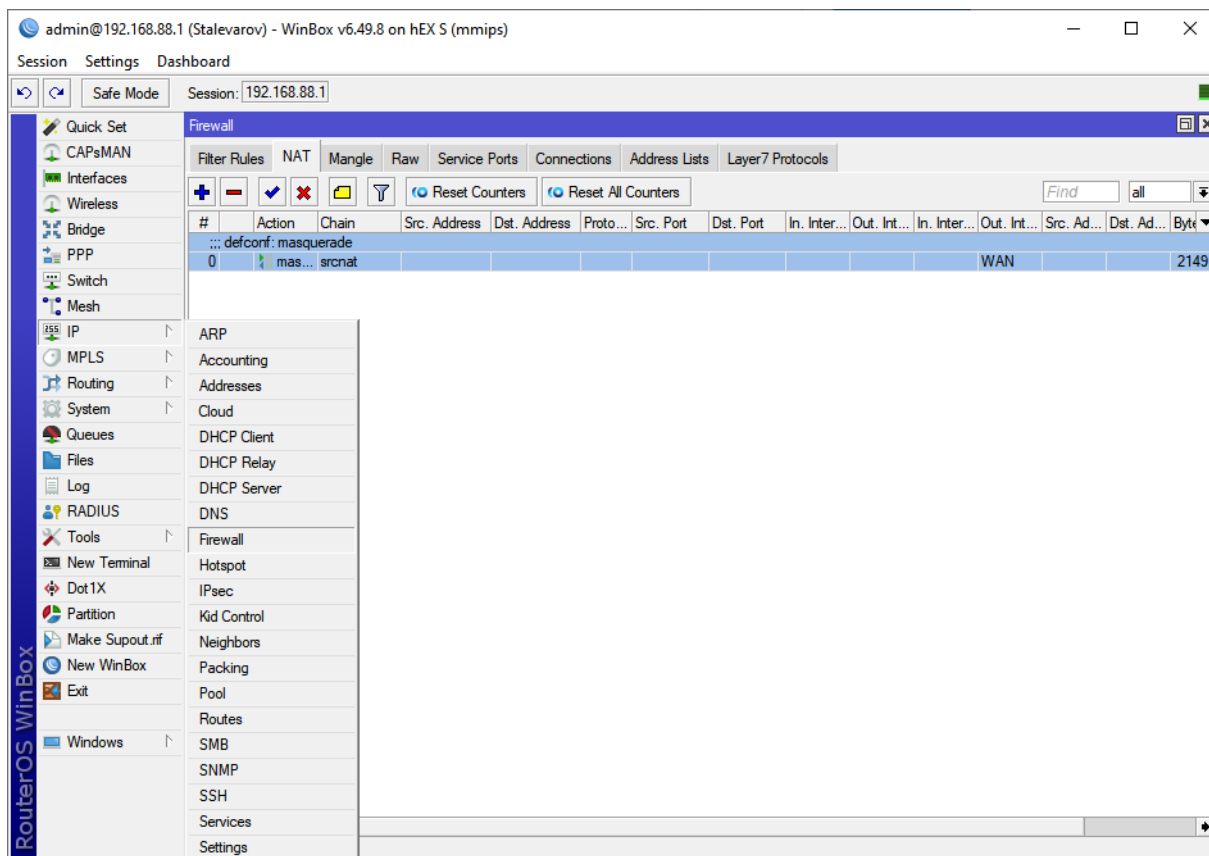
У каждой камеры есть два TCP-порта: 80 (протокол HTTP) и 554 (протокол RTSP). Необходимо на роутере настроить переадресацию портов так, чтобы соединения на TCP-порты из диапазона 10000-10999, открытые в VPN-соединении с InSentry.Cloud, попадали на 80 и 554 TCP-порты камер.

В процессе настройки переадресации придерживайтесь следующих правил:

- соединения с чётных портов из диапазона 10000-10998 необходимо перенаправлять на 80 порты камер (например, порт 10000 из VPN-соединения на 80 порт камеры);
- соединения со следующего по порядку нечетного порта необходимо перенаправлять на 554 порт той же камеры (например, порт 10001 из VPN-соединения на 554 порт камеры);
- для одного VPN соединения проброшенные порты на камеры не должны пересекаться — для каждой камеры должен быть свой индивидуальный порт.

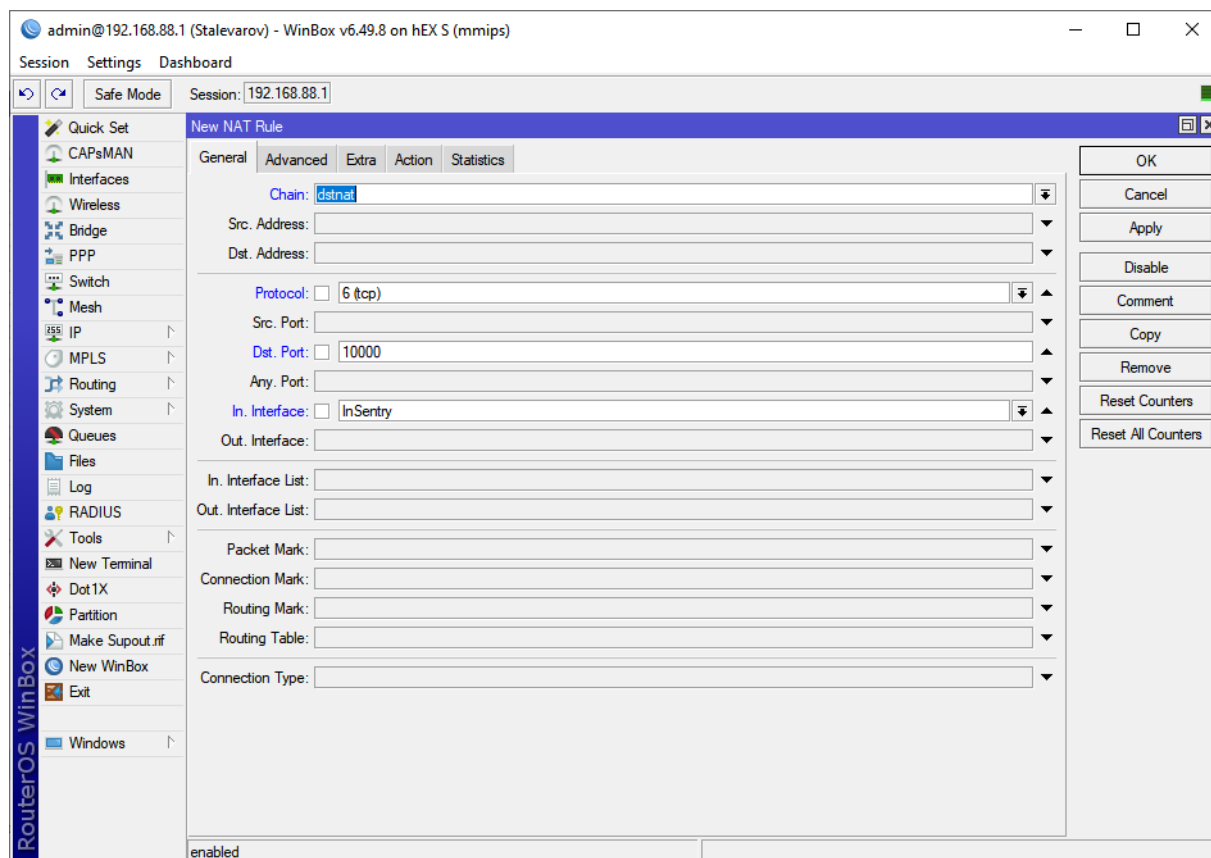
Для настройки переадресации:

1. Выберите пункт меню **IP → Firewall** и перейдите на вкладку **NAT**:

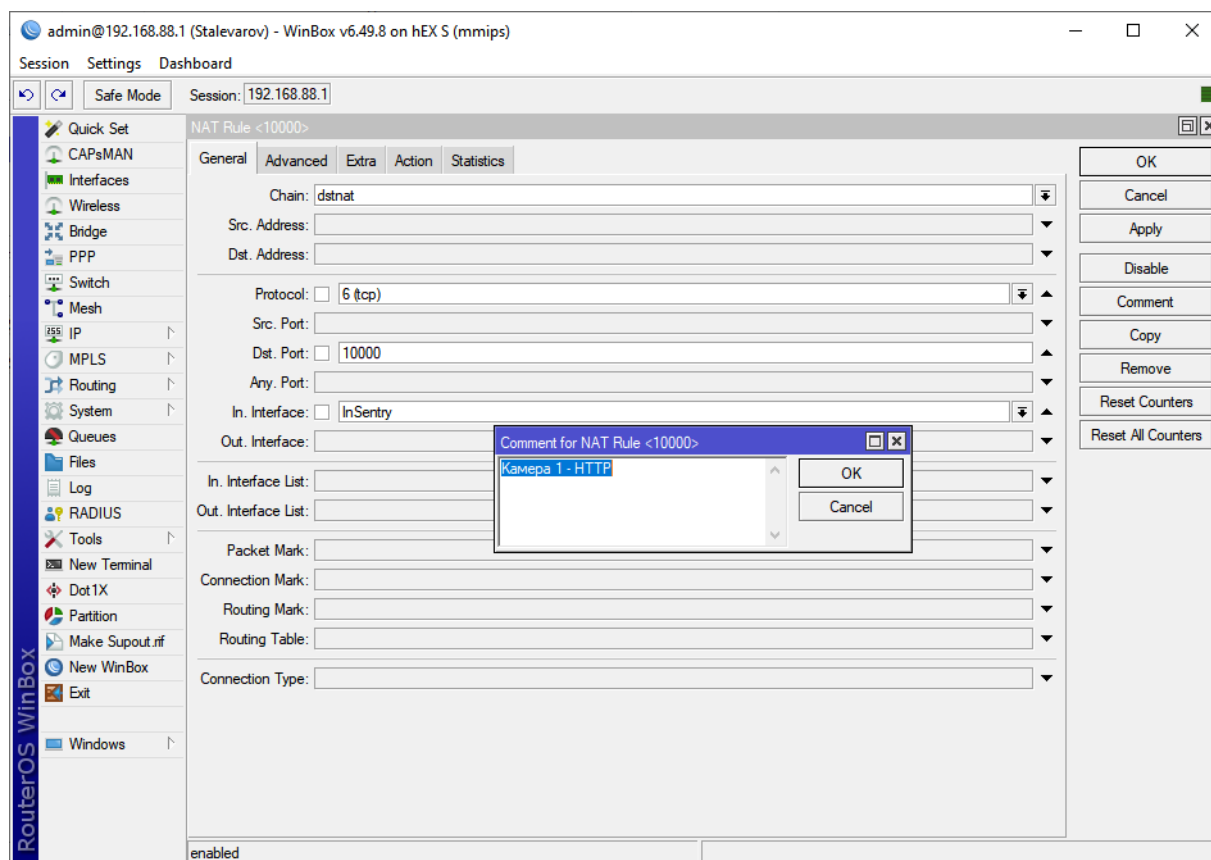


2. Нажмите «плюс» (+), откроется окно проброса порта. Перейдите на вкладку **General** и заполните поля:

- **Chain:** dstnat
- **Protocol:** 6 (tcp)
- **Dst. Port:** 10000
- **In. Interface:** InSentry



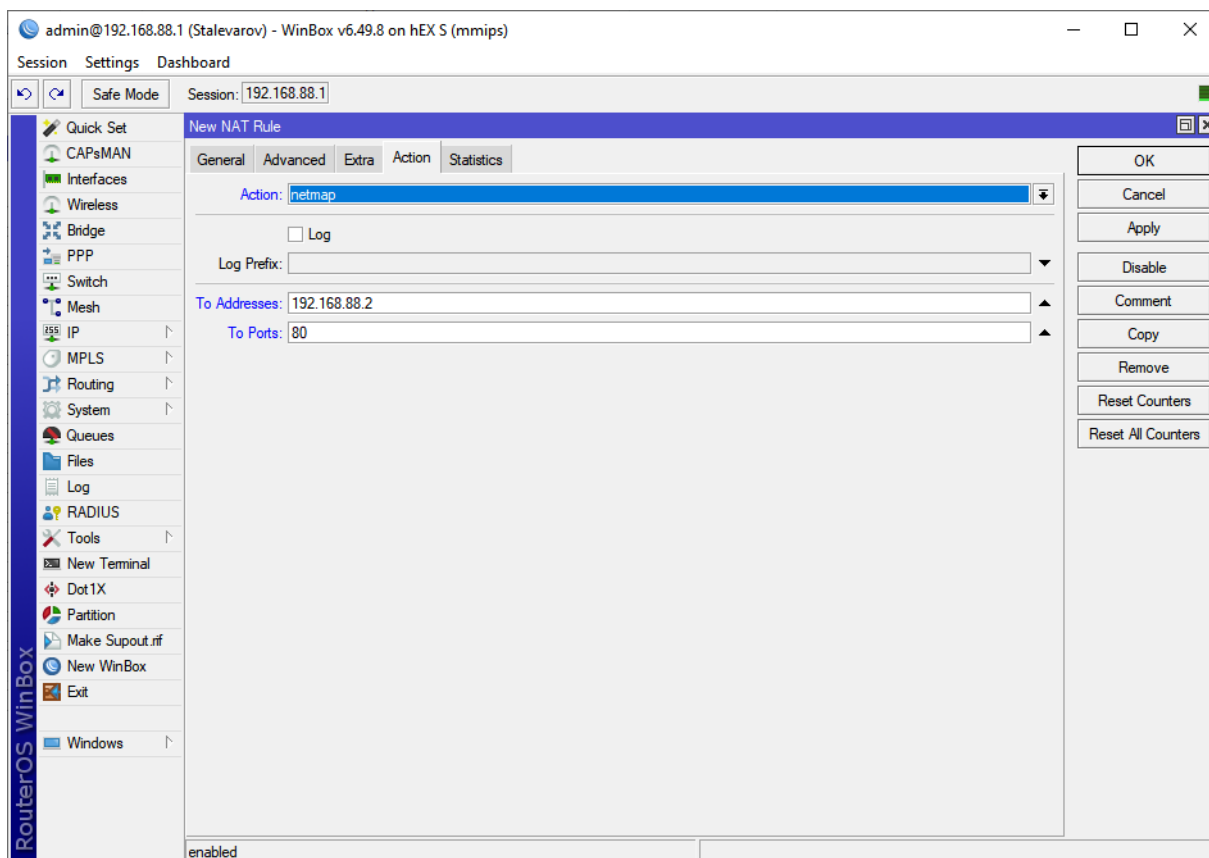
3. Нажмите **Apply** и затем **Comment**, введите название камеры и протокола: HTTP.



4. Перейдите на вкладку **Action** и заполните поля:

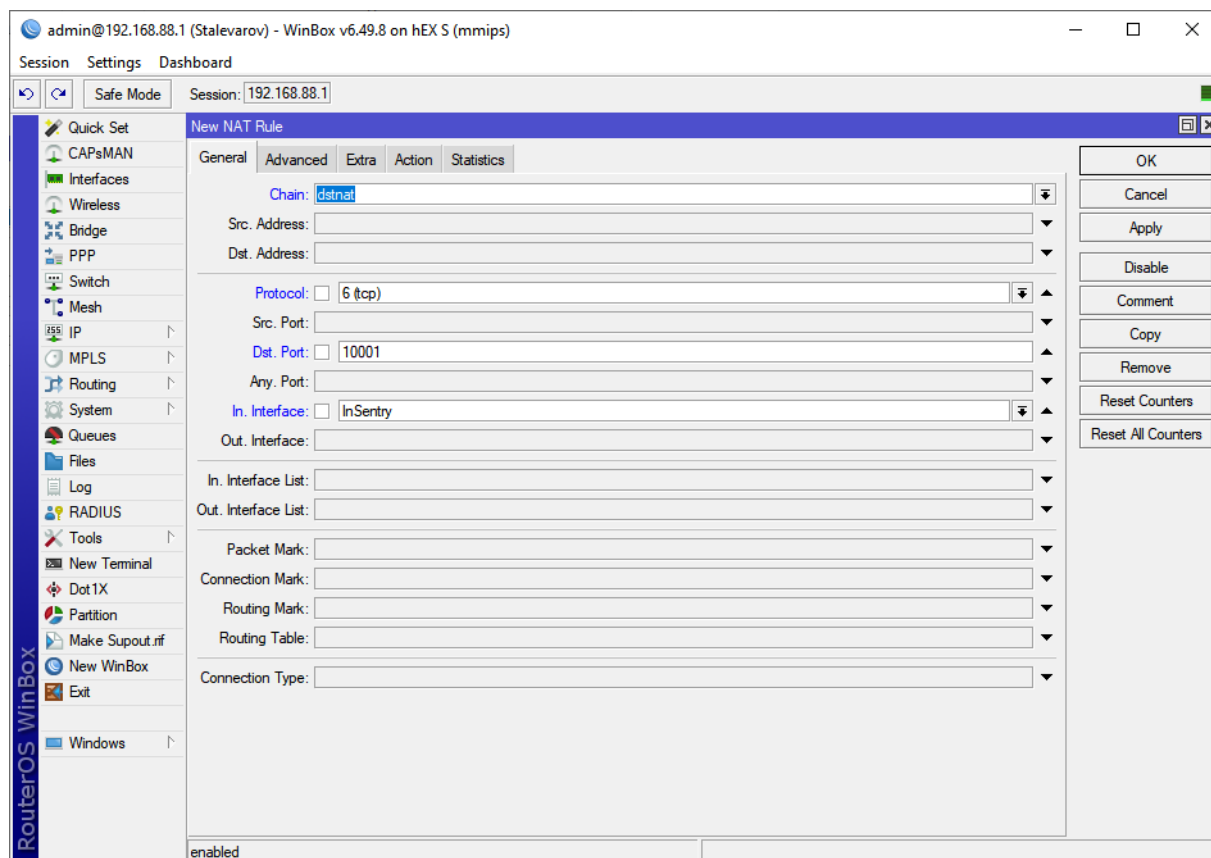
- **Action:** netmap
- **To Address:** IP-адрес камеры

- **To Ports:** 80

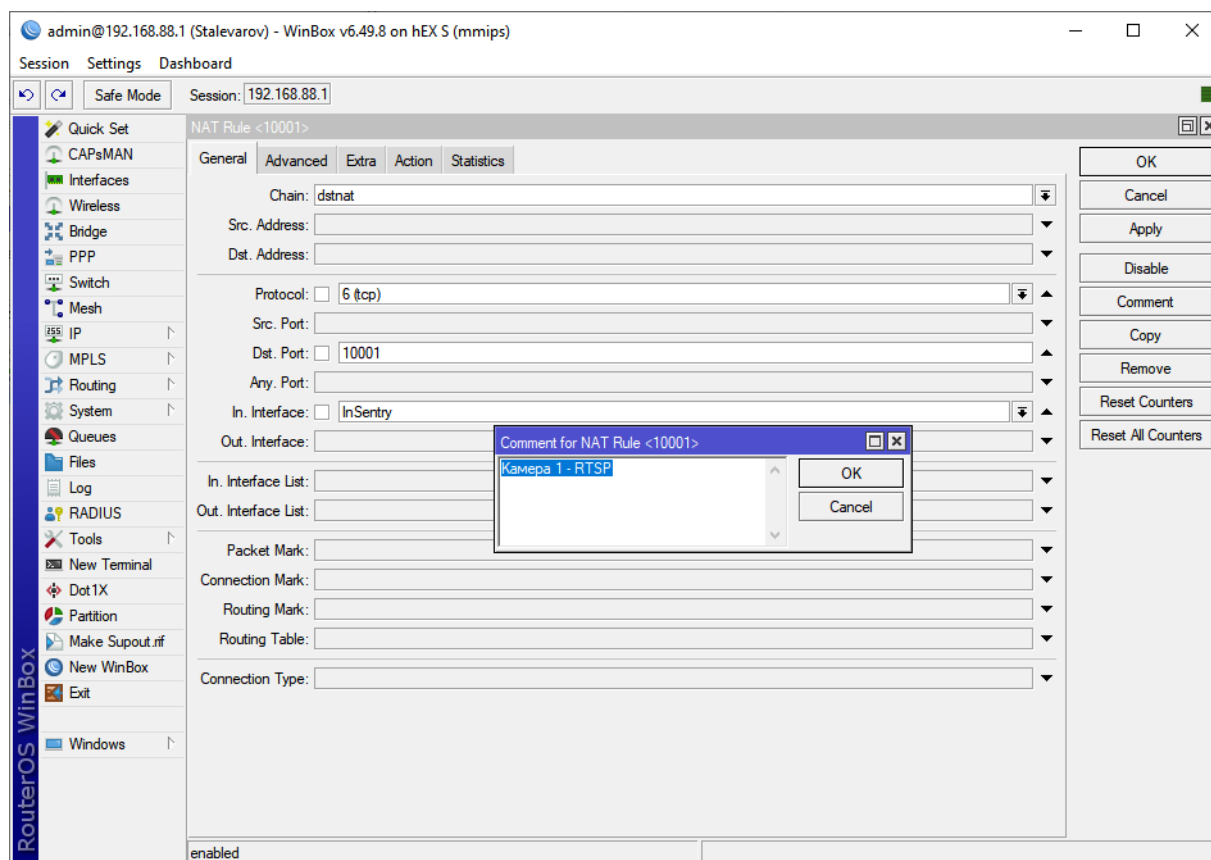


5. Нажмите кнопку **OK**, после чего аналогичным образом настройте переадресацию RTSP-порта той же камеры:

- **Chain:** dstnat
- **Protocol:** 6 (tcp)
- **Dst. Port:** 10001
- **In. Interface:** InSentry



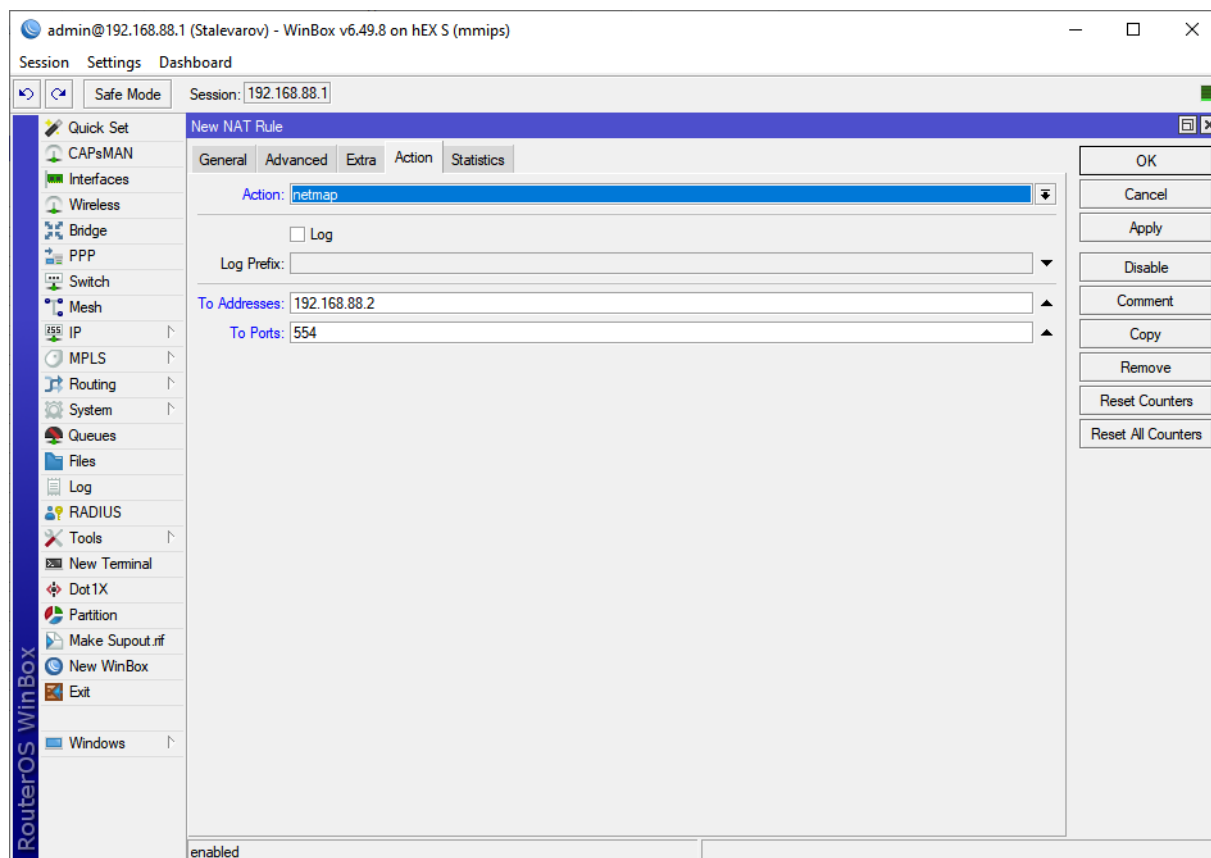
6. Нажмите **Apply** и затем **Comment**, введите название камеры и протокола: RTSP.



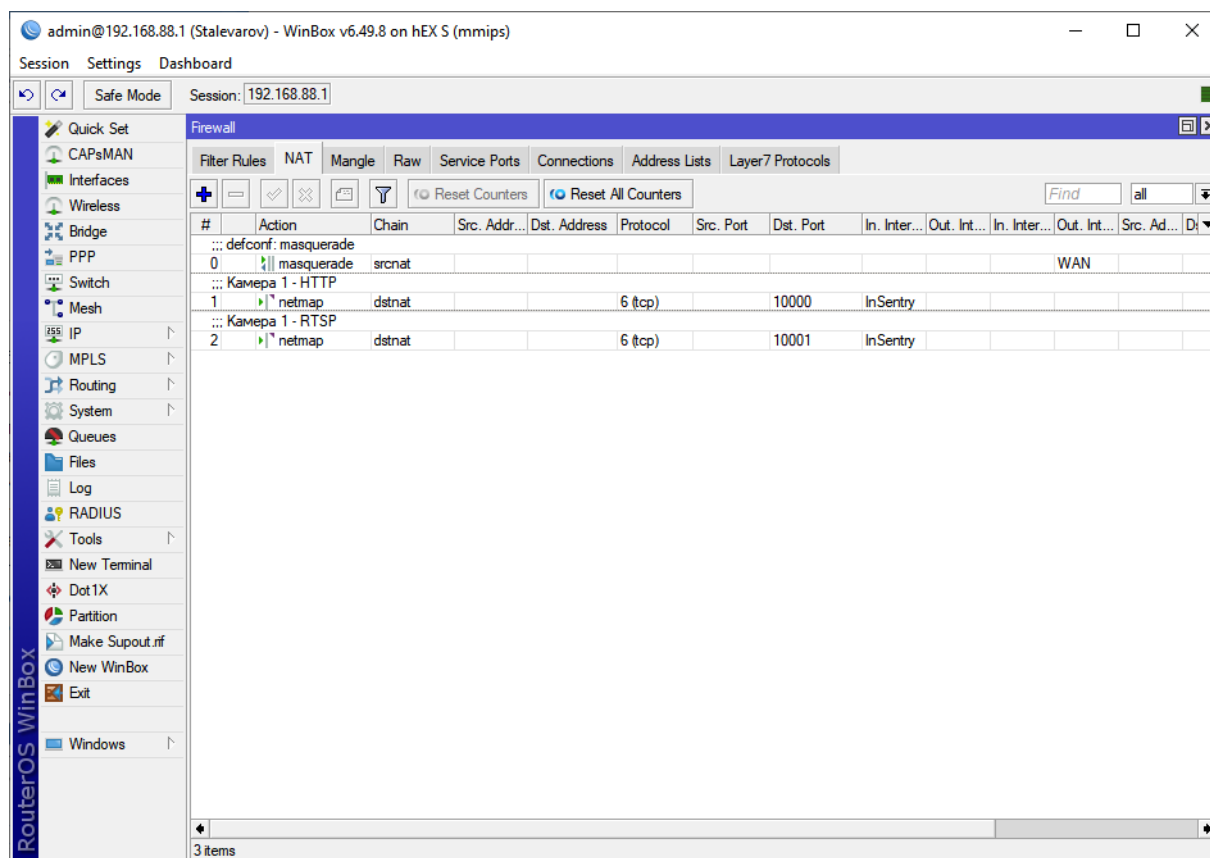
7. Перейдите на вкладку **Action** и заполните поля:

- **Action:** netmap
- **To Address:** IP-адрес камеры

- **To Ports: 554**



В результате настройки переадресации портов должны выглядеть следующим образом:



Если камер несколько, необходимо пробросить их порты аналогичным образом, используя другие номера портов из диапазона от 10000 до 10999.

Добавление камер из локальной сети через VPN

После того, как предыдущие шаги были завершены, OpenVPN-соединение с роутером активно и порты камер были успешно переадресованы в настройках роутера, можно приступать к подключению камер к облаку Insentry.

1. Откройте клиент Insentry на портале insentry.video.
2. В разделе **Управление → Устройства → Камеры → Мастер добавления**.
3. Укажите логин и пароль для доступа к камере.
4. Запустите проверку соединения.
5. Выберите одну или несколько из обнаруженных камер, успешно прошедших проверку, и нажмите **Добавить выбранные**.
6. Следуя шагам мастера добавления, завершите процесс.

После этого камеры будут подключены к облачной версии Insentry и доступны для просмотра на портале insentry.video.

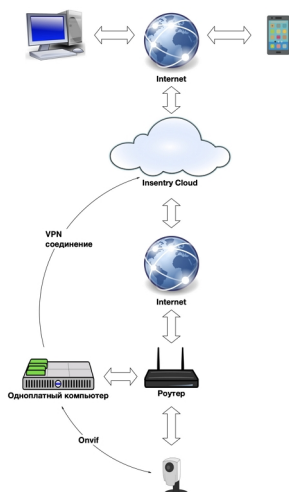
Подключение камер к Insentry.Cloud через одноплатный компьютер

Для подключения камер из локальной сети к Insentry.Cloud в роли роутера может быть использован компьютер под управлением операционных систем Windows или Linux, в том числе одноплатный компьютер Raspberry Pi, OrangePi и их аналоги.

Для реализации такого подключения требуется:

1. Настроить проброс портов.
2. Настроить VPN-соединение.
3. Подключить камеры.

Схема подключения:



Проброс портов

Для того, чтобы у Insentry.Cloud появился доступ к камерам, находящимся в локальной сети, необходимо настроить переадресацию HTTP и RTSP портов, доступных через VPN-соединение, на порты камер.

Составьте список IP-адресов камер, подключенных через роутер, которые необходимо подключить к Insentry.

У каждой камеры есть два TCP-порта: 80 (протокол HTTP) и 554 (протокол RTSP). Необходимо настроить переадресацию портов так, чтобы соединения на TCP-порты из диапазона 10000-10999, открытые в VPN-соединении с Insentry.Cloud, попадали на 80 и 554 TCP-порты камер.

В процессе настройки переадресации придерживайтесь следующих правил:

- соединения с чётных портов из диапазона 10000-10998 необходимо перенаправлять на 80 порты камер (например, порт 10000 из VPN-соединения на 80 порт камеры);
- соединения со следующего по порядку нечетного порта необходимо перенаправлять на 554 порт той же камеры (например, порт 10001 из VPN-соединения на 554 порт камеры);
- для одного VPN соединения сброшенные порты на камеры не должны пересекаться — для каждой камеры должен быть свой индивидуальный порт.

Фаервол должен быть настроен так, чтобы не блокировались никакие подключения к портам из диапазона 10000—10999 со стороны VPN-соединения: не только к сброшенным портам камер, а ко всему диапазону 10000—10999.

Для проброса портов используйте сервис Nginx. Способы установки Nginx:

- из репозитория используемого дистрибутива Linux (например, `sudo apt install nginx` для Ubuntu);
- в виде docker-контейнера, используя официальный образ Nginx (например, `sudo docker run --name nginx -v /host/path/nginx.conf:/etc/nginx/nginx.conf:ro -d nginx`);
- [скачать дистрибутив на официальном сайте nginx.org](https://nginx.org).

При любом способе установки потребуется составить файл конфигурации Nginx. Образец файла конфигурации Nginx (nginx.conf) для камеры с IP 192.168.0.10:

```
events {}
stream {
    server {
        listen      10000;
        proxy_pass  192.168.0.10:80;
    }
    server {
        listen      10001;
        proxy_pass  192.168.0.10:554;
    }
}
```

Если камер несколько, необходимо пробросить их порты аналогичным образом, используя другие номера портов из диапазона от 10000 до 10999.

Настройка VPN-соединения

1. Откройте клиент Insentry на портале insentry.video.
2. В разделе **Управление → Система → VPN-соединение** нажмите кнопку **Скачать** и сохраните zip-архив с файлом конфигурации VPN.
3. Установите клиент OpenVPN версии 2.6.0 и старше либо OpenVPN Connect 3.0 и старше:
 - на Linux — из репозитория (например, `sudo apt install openvpn` для Ubuntu);
 - на Windows — скачайте дистрибутив на официальном сайте [OpenVPN](https://openvpn.net) или [OpenVPN Connect](https://openvpn.net/connect).
4. Замените файл конфигурации по умолчанию файлом `insentry.ovpn`, скачанном на втором шаге. Для Linux-систем может потребоваться переименовать его в `client.conf`.

Внимание! В более ранних версиях OpenVPN при подключении может возникать ошибка:

```
Options error: Unrecognized option or missing or extra parameter(s) in
insentry.conf:28: auth-user-pass (2.4.12)
```

Причина этой ошибки в том, что ранние версии OpenVPN не поддерживают параметр `auth-user-pass` в теле файла конфигурации `insentry.ovpn`.

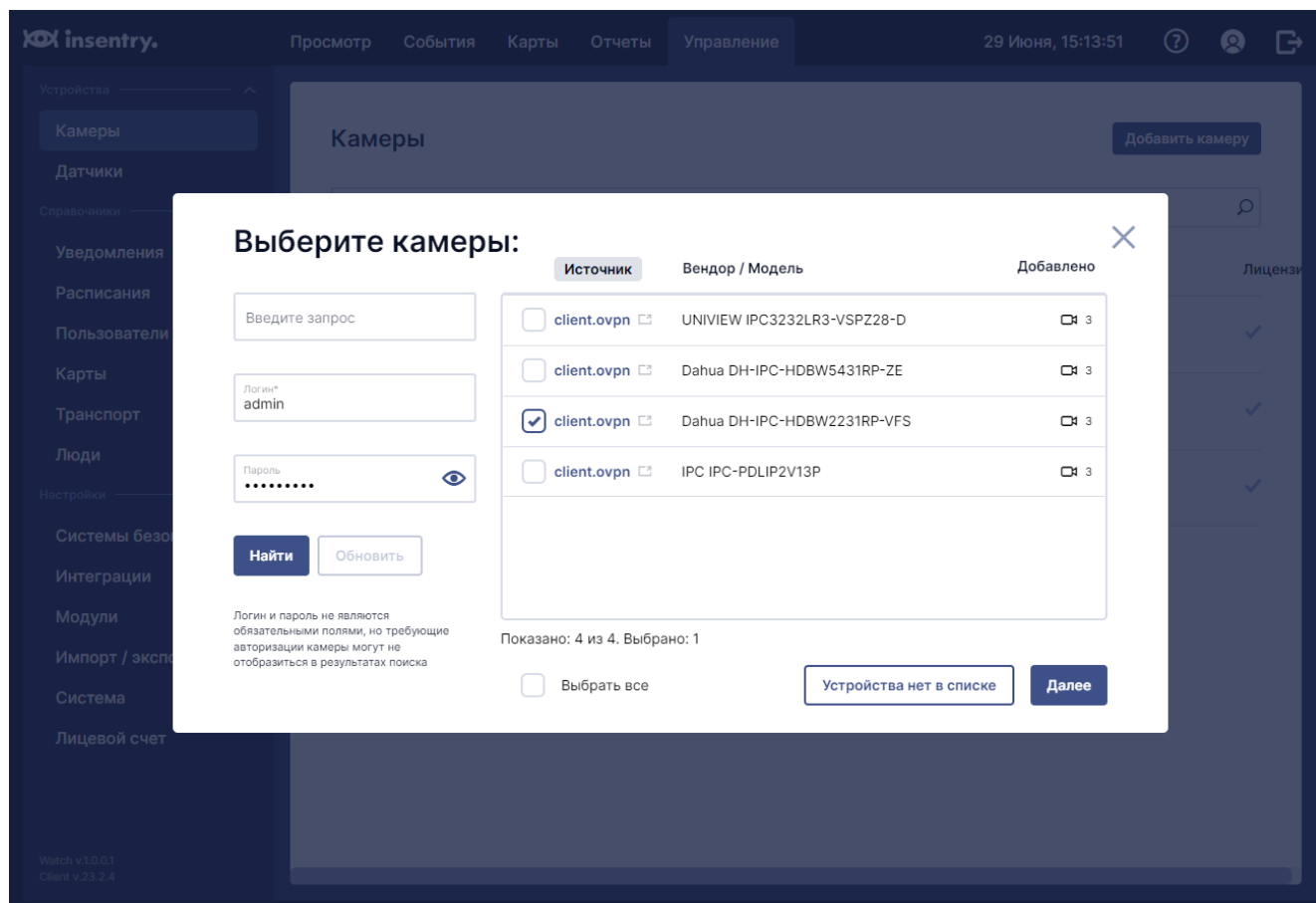
При возникновении ошибок соединения рекомендуется обновить клиент OpenVPN до актуальной версии. Если это невозможно: 1. Уберите раздел `auth-user-pass` из файла конфигурации. 2. Уберите точку с запятой из строки `;auth-user-pass pass.txt`. 3. Скопируйте файл `pass.txt` из архива в одну папку с файлом конфигурации.

Подключение камер из локальной сети к облаку Insentry

Если предыдущие шаги завершены, можно приступать к подключению камер.

1. Откройте клиент Insentry на портале insentry.video.
2. В разделе **Управление → Устройства → Камеры** нажмите кнопку **Добавить камеру**.
3. В открывшемся окне укажите логин и пароль для доступа к камере (они необходимы для опроса камеры через Onvif), а затем нажмите кнопку **Найти**. Поиск может занять продолжительное время.

Внимание! У некоторых моделей камер Onvif логин и пароль не совпадают с логином и паролем в панели администрирования камеры. Их нужно настраивать отдельно.



4. Выберите одну или несколько из обнаруженных камер и нажмите **Далее**.
5. Введите название камеры, нажмите **Далее** и завершите процесс добавления.

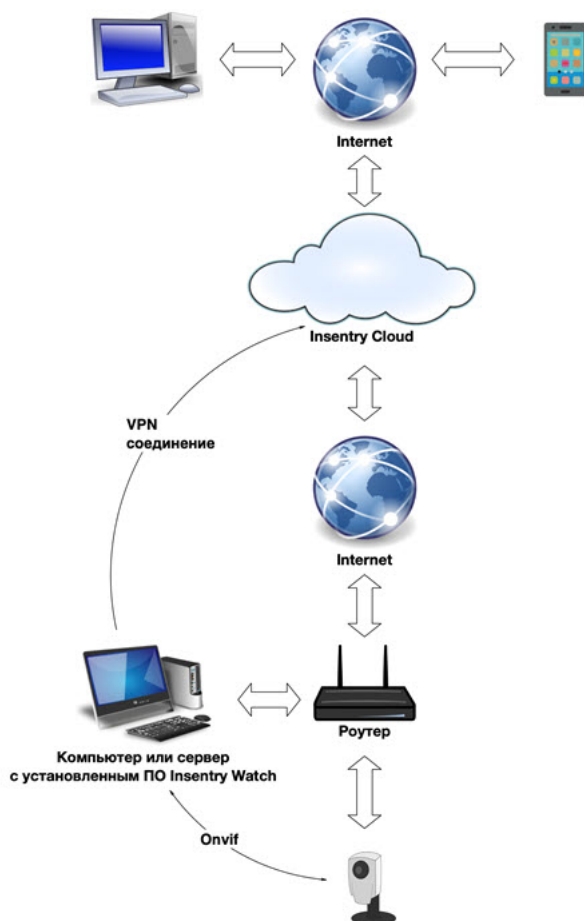
После этого камеры будут подключены к облачной версии Insentry и доступны для просмотра на портале insentry.video. Камеры из локальной сети будут доступны из Insentry.Cloud до тех пор, пока VPN-соединение активно.

Подключение камер к Insentry.Cloud с помощью Insentry.Watch

Insentry.Watch — серверная версия Insentry, которую вы можете установить на свой сервер или компьютер, после чего настроить передачу данных камер, подключенных к Insentry.Watch, в облако Insentry.Cloud. Если вы уже используете Insentry.Watch, такая настройка займёт несколько минут.

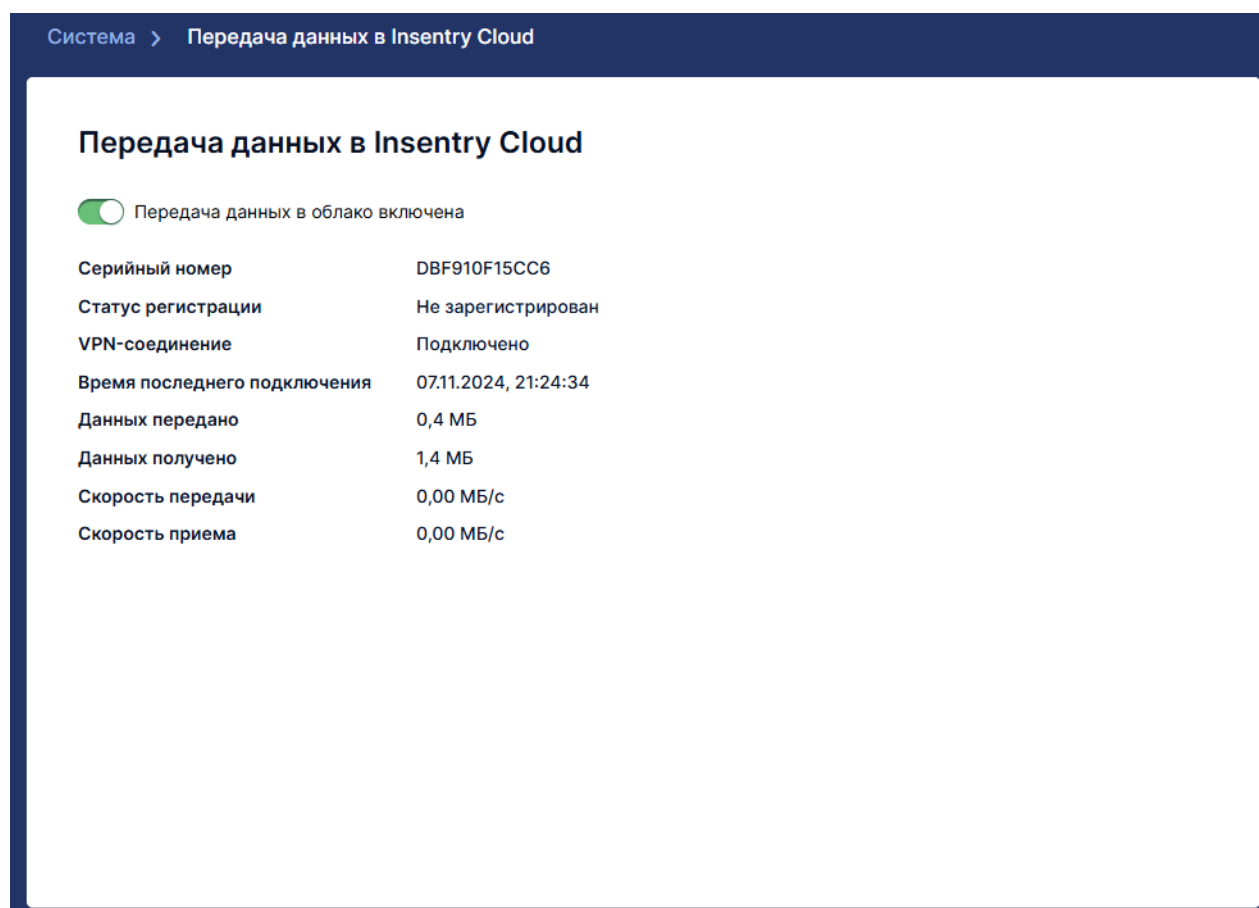
Если вы ещё не пользовались Insentry.Watch, то для начала работы с Insentry.Watch потребуется [получить лицензию](#) (платную или бесплатную) и [подключить камеры](#).

Схема подключения:



Настройка передачи данных с камер, подключенных к серверной версии Insentry.Watch, в облако Insentry:

- 1) В интерфейсе Insentry.Watch в разделе **Система → Передача данных в Insentry Cloud** включите передачу данных в облако. Когда статус VPN-соединения изменится на «Подключено», переходите к следующему шагу.



Если возникает ошибка «TAP адаптер недоступен», попробуйте перезапустить соединение, а если это не поможет, обратитесь в техподдержку.

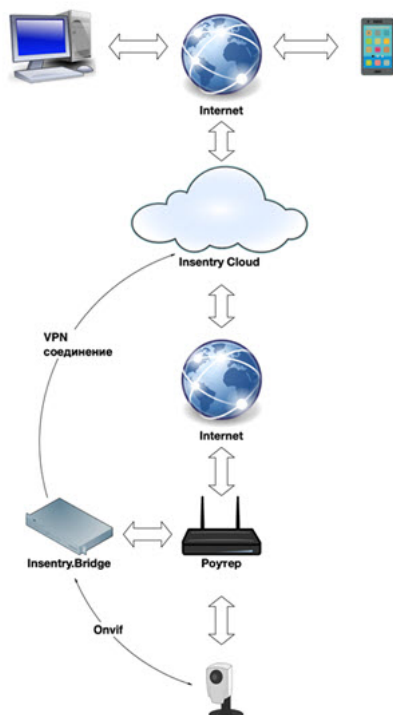
- 2) В том же окне скопируйте серийный номер и укажите его в разделе **Управление → Insentry.Bridge** в интерфейсе облака на сайте insentry.video. Дождитесь, пока статус подключения изменится на «Активно».
- 3) В интерфейсе Insentry.Watch в разделе **Система → Передача данных в Insentry Cloud** проверьте, что статус VPN-соединения изменился на «Зарегистрирован» — это означает, что серверная инсталляция Insentry.Watch теперь привязана к вашему аккаунту в облаке.
- 4) В [настройках камер](#), данные которых вы хотите передавать в облако, включите параметр **Транслировать в Insentry.Cloud**.
- 5) Убедитесь, что камеры появились в списке камер на сайте insentry.video. Теперь вы сможете просматривать видео с этих камер в интерфейсе облака Insentry. Если на камерах, добавленных в облако, записывается локальный архив, то он доступен для просмотра в облаке.

Подключение камер к Insentry.Cloud с помощью Insentry.Bridge

Insentry.Bridge — одноплатный компьютер, на котором уже установлено ПО для работы с облаком Insentry. Когда Insentry.Bridge подключится к вашей сети, он найдёт камеры автоматически по протоколу ONVIF, и вы сможете начать использовать облачное видеонаблюдение Insentry без дополнительных настроек.

Чтобы приобрести одноплатный компьютер Insentry.Bridge, обратитесь в отдел продаж: sales@insentry.io.

Схема подключения:



Регистрация Insentry.Bridge

Включите устройство Insentry.Bridge в сеть. Программное обеспечение, необходимое для подключения к Insentry, на нём уже установлено. Нужно только подключить Insentry.Bridge к облачной версии ПО Insentry, а затем подключить камеры к облаку — они будут обнаружены автоматически.

Чтобы подключить Insentry.Bridge:

1. Включите Insentry.Bridge и активируйте на нём Wi-Fi.
2. Зарегистрируйтесь на портале insentry.video. Оформите платную или бесплатную подписку.
3. Перейдите в раздел меню **Управление → Insentry.Bridge**.
4. Нажмите кнопку **Добавить**.
5. Укажите серийный номер Insentry.Bridge, состоящий из 12-ти шестнадцатеричных символов. Номер указан на самом устройстве.
6. Нажмите кнопку **Сохранить**. Если указан верный серийный номер, Insentry.Bridge появится в списке.
7. Подождите несколько секунд, пока Insentry.Bridge подключится. Как только подключение будет установлено, в столбце **Статус подключения** появится статус **Активно**.

Устройства Insentry.Bridge				Добавить
Серийный номер	Статус подключения	Время последнего подключения	IP-адрес	
0050B65BCA6A	Активно	15.05.2023, 15:30	123.242.95.01	Настройки
0050B65BCA6A	Активно	15.05.2023, 15:30	123.242.95.01	Настройки
0050B65BCA6A	Неактивно	15.05.2023, 15:30	123.242.95.01	Настройки

Сетевые настройки Insentry.Bridge

Откройте веб-интерфейс Insentry.Bridge:

- указав его IP-адрес в адресной строке браузера;
- нажав кнопку **Настройки** в списке подключенных устройств в разделе **Управление** → **Insentry.Bridge** на портале insentry.video.

insentry.

29 апреля, 15:40:16

ONVIF камерыДругие камерыНастройки

Информация

Серийный номер

0050B65BCA6A

Статус регистрации

Зарегистрирован

VPN-соединение

Установлено

Время последнего подключения

15.05.2023, 15:40

Данных передано

0 МБ

Данных получено

0 МБ

Скорость передачи

2.1 МБ/с

Скорость приема

2.1 МБ/с

Сетевые настройки

☐ IP адрес определяется автоматически

IP адрес

192.168.12.01

Маска подсети

255.255.255.0

Шлюз по умолчанию

255.255.255.0

DNS 1

192.168.1.1

DNS 2

Не задано

Сохранить

Игнорируемые диапазоны адресов ONVIF

172.17.12.0/24

172.17.12.1/24

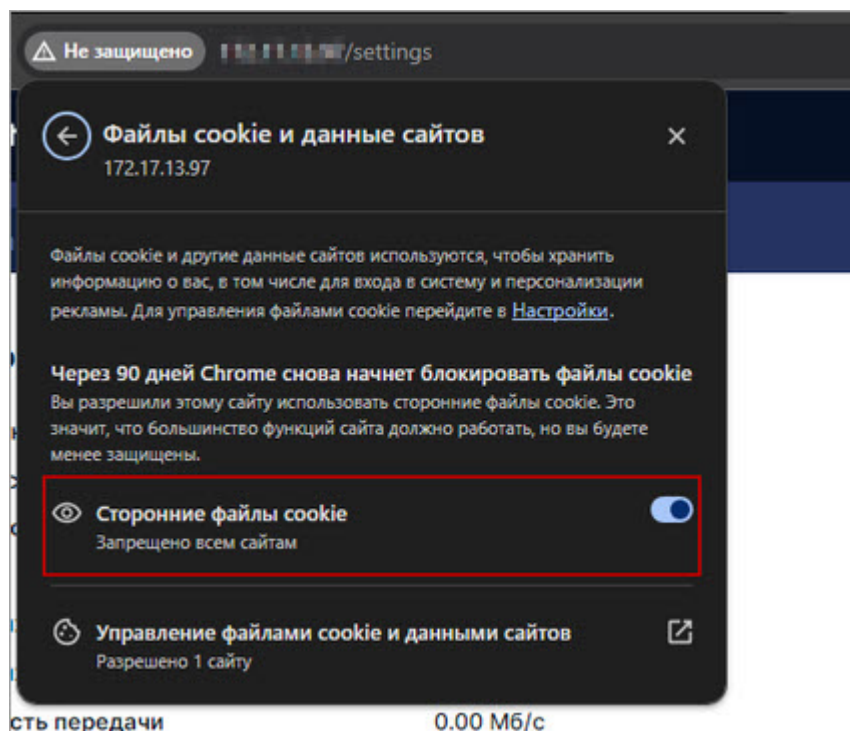
+

В правой части окна задайте сетевые настройки:

- IP адрес определяется автоматически** — включите настройку, если используете DHCP для автоматического назначения IP адресов устройствам в вашей сети. Если вы задаёте адреса устройств вручную, укажите адрес подключенного устройства Insentry.Bridge, маску подсети, шлюз и адреса DNS в полях ниже.

- **Игнорируемые диапазоны адресов ONVIF** — добавьте сюда адреса подсетей, которые вы хотите игнорировать при поиске камер по протоколу ONVIF. Адреса сетей должны быть указаны в формате `192.168.1.0/24`.

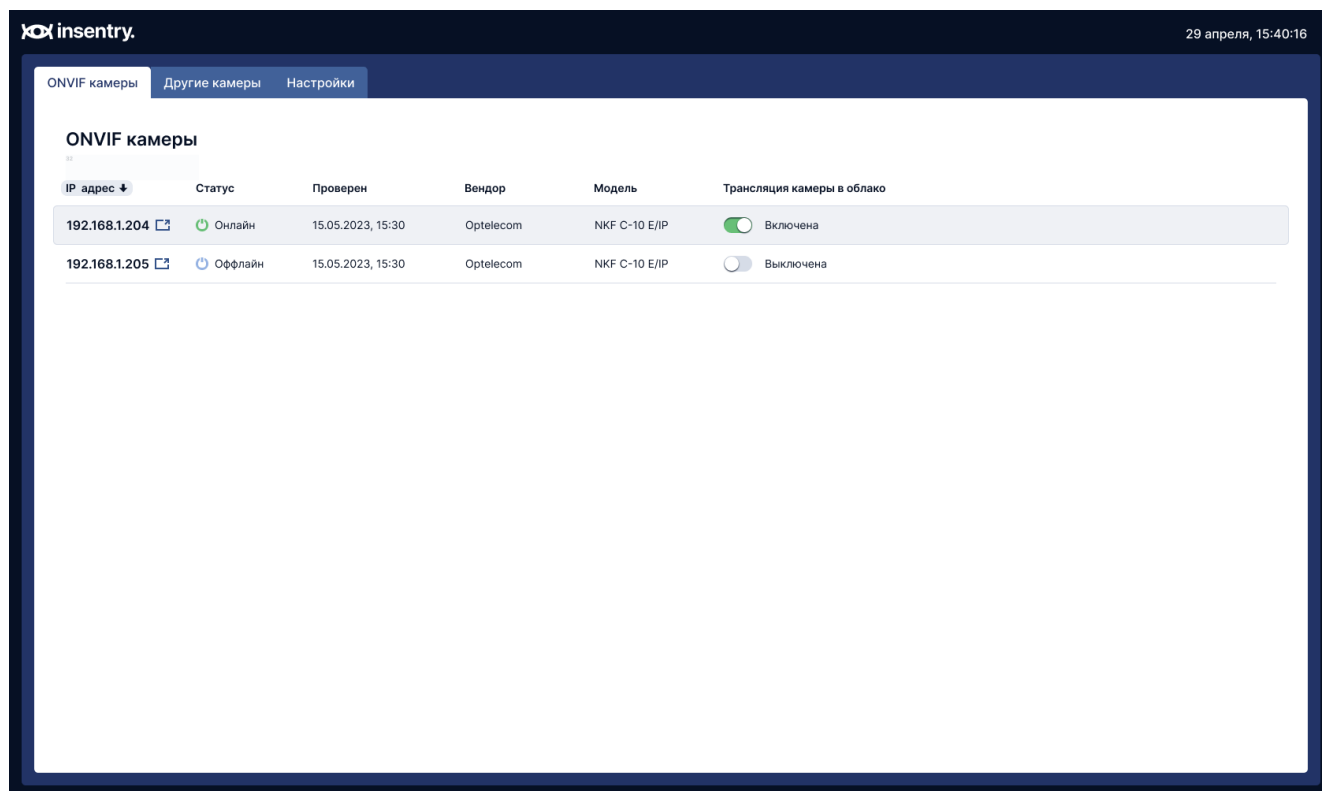
Если Insentry.Bridge появился в списке устройств в облаке, а на самом устройстве продолжает отображаться плашка «Авторизуйтесь», то разрешите сторонние куки:



Подключение камер через Insentry.Bridge

Когда Insentry.Bridge зарегистрирован, можно приступать к подключению камер:

1. Подключите камеры к сети.
2. В веб-интерфейсе Insentry.Bridge перейдите в раздел **Управление** → **Insentry.Bridge** → **ONVIF камеры**.
3. Проверьте, что в списке появились камеры, поддерживающие протокол ONVIF.



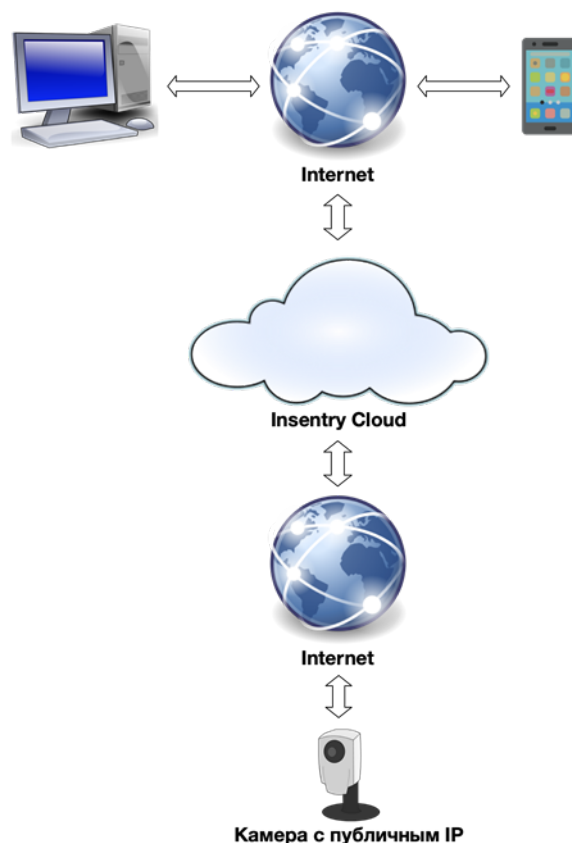
Настройка **Трансляция в облако** отвечает за то, чтобы камера транслировала видеопоток в облако Insentry. Если камера добавлена, но трансляция отключена, камера не будет видна в списке камер при работе с ПО Insentry.

4. Если камера не поддерживает ONVIF, перейдите на вкладку **Другие камеры** и добавьте камеру вручную, указав её адрес и порты для доступа по протоколам HTTP и RTSP (по умолчанию это 80-й и 554-й порты соответственно).
5. В веб-интерфейсе Insentry на портале insentry.video перейдите в раздел **Управление → Устройства → Камеры**.
6. Добавьте камеры [по инструкции](#). Обратите внимание, что у камер, подключенных через Insentry.Bridge, в окне добавления камер вместо IP-адреса будет отображаться серийный номер устройства.

Подключение к Insentry.Cloud камер с публичным IP

Если камеры со статическим публичным IP подключены к сети напрямую, без роутера, то их можно добавить в облако по IP-адресу.

Схема подключения:



Порядок настройки:

1. На портале insentry.video перейдите в раздел **Управление → Устройства → Камеры → Мастер добавления**.
2. Нажмите в окне поиска камер кнопку **Камеры нет в списке**.
3. Укажите параметры камеры в полях формы, в том числе, логин и пароль для доступа к видеопотоку камеры.
4. Укажите настройки портов камеры, заполнив поля номерами соответствующих портов:

- * HTTP (порт по умолчанию «80»);
- * RTSP (порт по умолчанию «554»);
- * Onvif (порт по умолчанию «80»).

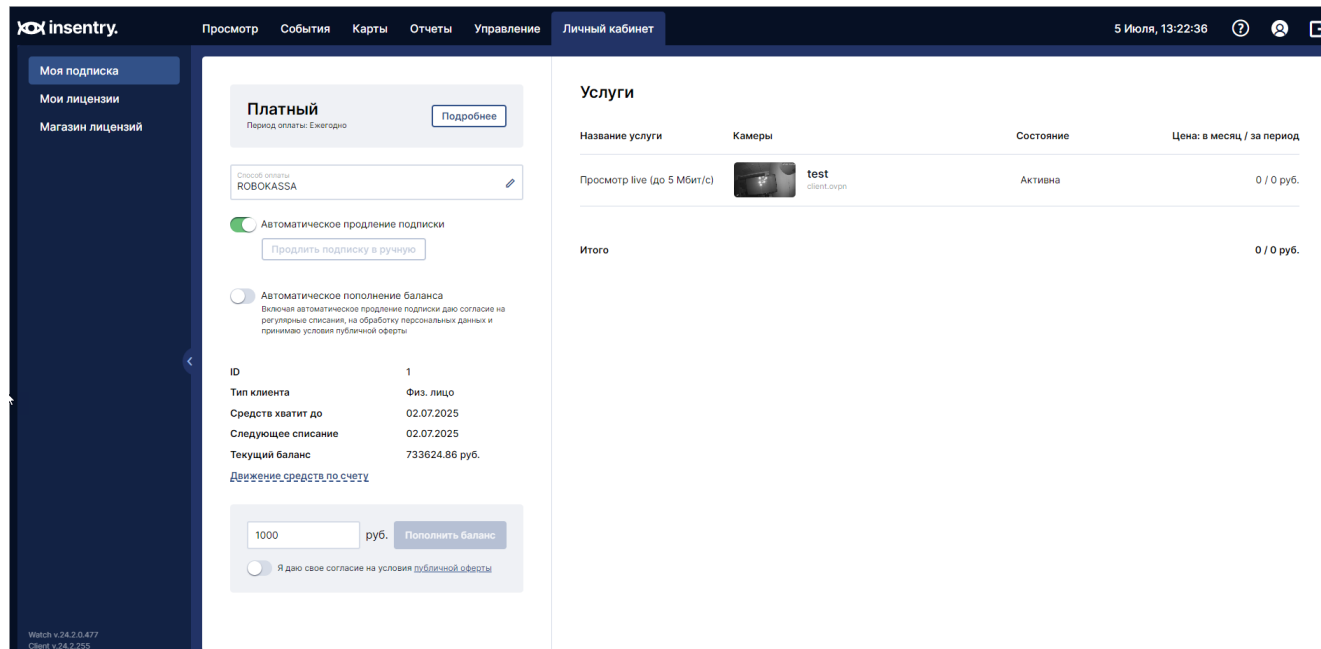
4. Продолжите выполнение операции, следуя указаниям мастера добавления.

Даже если вы используете камеры с белым статическим IP, лучше настроить на роутере VPN, чтобы ограничить несанкционированный доступ. Подключать камеры напрямую без роутера не рекомендуется.

См. также: [Подключение камер к Insentry.Watch](#)

Управление подпиской

Управление подпиской производится на портале insentry.video в разделе **Личный кабинет** → **Моя подписка**.



В левой части экрана представлены:

- название текущего тарифа и кнопка **Подробнее** для смены тарифа;
- блок выбора метода оплаты;
- настройки автоматического продления подписки и пополнения баланса;
- информация о текущем балансе и движении средств по счёту;
- блок пополнения баланса.

В правой части экрана представлен перечень услуг, включённых в текущий тариф, с детализацией по состоянию услуги и стоимости за период.

Просмотр информации о тарифах. Смена тарифа

Чтобы просмотреть информацию о выбранном тарифе или сменить тариф, нажмите кнопку **Подробнее** в правой верхней части экрана. Будет представлен калькулятор тарифов, где вы можете ввести нужные вам значения для расчёта стоимости видеонаблюдения и облачного архива.

Чтобы сменить тариф, нажмите кнопку **Выбрать** в колонке нужного тарифа.

Тарифный план

Бесплатный Платный

Подписка 30 дней

Подписка 90 дней

Подписка 365 дней

По мере использования

Калькулятор расчёта стоимости видеонаблюдения за одну камеру

Каждый день 60 минут трансляции видео с камеры в одном слоте предоставляются бесплатно. Если камеру смотрят в двух слотах или два пользователя, бесплатная трансляция закончится за 30 минут. Дальнейшая трансляция оплачивается согласно тарифу.

Битрейт, Mbit/s

3

Часов трансляция в сутки

1

~0 Р в день

~0 Р в день

~0 Р в день

~0 Р в день

Периодичность списания ?

Ежедневно

Ежедневно

Ежедневно

Ежедневно

Калькулятор расчёта стоимости облачного видеоархива за одну камеру

В подписках 30/90/365 дней указана стоимость постоянной записи в облачный архив для одной камеры при предварительной оплате полной длительности подписки.

Битрейт, Mbit/s

3

Глубина хранения, дней

7

~21.67 Р в день

~20.17 Р в день

~18.44 Р в день

До 25.32 Р ? в день

Периодичность списания

30 дней ~ 651 Р за период

90 дней ~ 1816 Р за период

365 дней ~ 6731 Р за период

Ежедневно

Подробнее информацию о тарифных планах вы можете найти на нашем сайте

Выбрать

Выбрать

Текущая подписка

Выбрать

[Подробнее описание тарифов на сайте →](#)

Пополнение баланса

Чтобы пополнить баланс:

1. Выберите способ оплаты в поле **Способ оплаты**.
2. Ознакомьтесь с [публичной офертой](#).
3. Установите отметку в поле **Я даю свое согласие на условия публичной оферты**.
4. Введите сумму, на которую вы хотите пополнить баланс.
5. Нажмите кнопку **Пополнить баланс**. В отдельной вкладке будет выполнена переадресация на сайт платёжного шлюза в зависимости от выбранного способа оплаты.
6. Произведите оплату.
7. Дождитесь, пока деньги будут зачислены на счёт, и баланс в разделе **Личный кабинет** обновится.

Запись и хранение архива в облаке

Если на камерах, которые передают данные из серверной версии Insentry.Watch в облако Insentry.Cloud, записан локальный архив, то он доступен для просмотра в интерфейсе облачной версии. Если включена запись архива в облаке, то просмотр локального архива в облаке будет недоступен. На каждой камере доступен либо локальный, либо облачный архив.

Чтобы включить запись и хранения архива в облаке на камерах, подключенных непосредственно в облако, нужно создать правило записи архива в интерфейсе облачной версии на сайте [insentry.video](#).

Деньги за услугу хранения облачного архива списываются с лицевого счёта не при оформлении подписки, а после начала записи архива на камере (сохранения правила записи). Правило записи архива можно добавить в настройках камеры (**Управление → Устройства → Камеры → Настройки камеры → Архив**).

Настройки Права Теги **Архив** Видеоаналитика Связанные объекты

Правило записи

Хранилище/Поток

S3 storage
1280x720@10fps, H264

Новое правило записи ✕

Хранилище
S3 storage

Поток
704x576@10fps, H264

Лимит (суток)
7

Услуга
Запись видео в архив до 0.5 Мбит/сек глубины 7 дней. (рублей за камеру/м...

Стоимость руб/месяц	Сейчас будет списано (рублей)	Дата следующего списания абонентской платы
2068.33	2022.68	02 июля 2025

☒ Включить запись

Отмена Сохранить

При изменении действующего правила записи деньги будут возвращены либо списаны с лицевого счёта в зависимости от того, как меняется правило записи.

Выбирайте битрейт не ниже минимального, поддерживаемого камерой

Для подписок 30/90/365 дней: если камера пишет архив с битрейтом, превышающим указанный в описании услуги, то глубина архива будет уменьшена пропорционально разнице в заявленном и фактическом битрейтах. Например, если выбрана услуга записи архива с битрейтом 1 МБ/с и глубиной хранения 5 дней, а камера записывает архив с битрейтом 5 МБ/с, то глубина хранения архива в облаке составит 1 день.

При отключении камер от облака, облачных архив стирается без возможности восстановления.

См. также: [Запись архива в Insentry.Watch](#)

Управление учётными записями

Учётные записи пользователей облачной версии Insentry создаёт администратор в разделе **Управление → Пользователи**. Логины пользователей уникальны.

После авторизации в Insentry.Cloud со логином и паролем, выданными администратором, пользователь будет видеть камеры, к которым администратор предоставил ему доступ.

См. также:

- [Создание учётной записи](#)
- [Настройка прав доступа](#)

Отключение камер от облака

Камеры, [подключенные через Insentry.Watch](#), отключаются от облака при отключении их от серверной версии Insentry.

Камеры, [подключенные через Bridge](#), отключаются от облака при удалении Bridge в разделе Insentry.Bridge.

Камеры, подключенные через роутер, отключаются от облака при удалении VPN-соединения, с помощью которого они были добавлены (**Управление → Система → VPN-соединения**).

При отключении камер от облака, облачный архив стирается без возможности восстановления.