
FindFaceSecurity

Выпуск 1.2.1

NtechLab

июн. 26, 2023

Содержание

1	Полное руководство	1
1.1	Руководство администратора	1
1.2	Руководство оператора	35
1.3	Интеграция с партнерами	50

Система распознавания лиц FindFace Security предназначена для автоматизации основной деятельности сотрудников служб безопасности и гостеприимства и может использоваться в таких областях, как транспорт, розничная торговля, банковское обслуживание, индустрия развлечений, спортивные мероприятия, организация мероприятий, сервисы знакомств, видеонаблюдение, общественная и корпоративная безопасность.

Работа FindFace Security основывается на биометрической видео-идентификации, т. е. на распознавании лиц на видеоизображении в режиме реального времени. FindFace Security распознает лица нежелательных персон и VIP-гостей и оповещает сотрудников служб безопасности и гостеприимства об их приходе.

Раннее распознавание прихода нежелательных персон и VIP-гостей позволяет решать следующие задачи:

- снижение операционных потерь от мошеннических действий;
- снижение репутационных потерь и предотвращение конфликтных ситуаций;
- повышение качества обслуживания клиентов, в частности VIP-гостей;
- предотвращение потенциально опасных ситуаций, угрожающих жизни и здоровью людей.

FindFace Security supports the integration of third-party solutions.

Настоящий документ предназначен для администраторов, операторов и пользователей FindFace Security. Он также будет полезен специалистам, обслуживающим систему и ее комплекс технических средств.

1.1 Руководство администратора

1.1.1 Архитектура

FindFace Security разворачивается на одиночном сервере или нескольких серверах.

Совет: См. *Системные требования*.

Работоспособность FindFace Security обеспечивается взаимодействием следующих компонентов:

Компонент	Описание
PostgreSQL	База данных (СУБД), в которой хранятся детализированные досье персон с разбиением по категориям (спискам наблюдения), биометрические данные персон, а также все события распознавания лиц. Помимо этого, в базе данных хранится информация внутреннего характера: профили пользователей FindFace Security, данные видеоканера и пр.
ffsecurity	Сервис, который связывает воедино все компоненты FindFace Security, обеспечивая функционирование системы. Включает в себя сервисы <code>findface-security-proto</code> (отвечает за HTTP и web-socket) и <code>findface-security-worker</code> (обеспечивает взаимодействие остальных компонентов системы). Получает от сервиса <code>video-worker</code> нормализованное изображение, полный кадр и мета-данные обнаруженного лица. Перенаправляет нормализованное изображение лица в сервис <code>extraction-api</code> для извлечения биометрического образца. Полученный биометрический образец используется для поиска наиболее схожих лиц в списках наблюдения с помощью сервиса <code>findface-postgres-facen</code> . После этого событие обнаружения лица записывается в базу данных PostgreSQL вместе с результатом поиска и отображается в веб-интерфейсе. Сервис <code>ffsecurity</code> также отвечает за поиск лиц в базе событий и базе досье.
videomanager-api	Сервис, являющийся частью модуля видеодетекции лиц, через который осуществляется управление детекцией лиц на видео, а именно задаются настройки и список видеопотоков для обработки. Взаимодействует с сервисом <code>video-worker</code> .
video-worker	Сервис, являющийся частью модуля видеодетекции лиц, который обнаруживает лицо «на лету» в видеопотоке или видеофайле и отправляет его нормализованное изображение, полный кадр и мета-данные, такие как ID камеры и метку времени обнаружения, в сервис <code>ffsecurity</code> .
extraction-api	Сервис, который используется для извлечения биометрического образца (вектора признаков) лица.
findface-postgres-facen	Расширение к базе данных PostgreSQL, которое используется для вычисления степени схожести обнаруженного лица с лицами из досье путем сравнения биометрических образцов.
ffsecurity-ui	Веб-интерфейс используется для отображения результатов работы системы распознавания лиц, управления видеоканерами, пользователями, ведения списков наблюдения, поиска лиц в базе событий и досье.
NTLS	Локальный сервер лицензий с управлением через веб-интерфейс, взаимодействующий для верификации лицензий с глобальным сервером лицензий NtechLab или аппаратным лицензионным ключом.
etcd	Стороннее программное обеспечение, реализующее распределенное хранилище ключей для компонента <code>videomanager-api</code> . Используется в качестве координационной службы в распределенной системе, обеспечивая отказоустойчивость модуля видеодетекции лиц.

Примечание: Работа с FindFace Security выполняется через веб-интерфейс.

1.1.2 Системные требования

Для расчета характеристик сервера развертывания FindFace Security используйте следующие требования:

Требование	Описание
Процессор	Intel Xeon E5 с поддержкой AVX или аналогичный ему процессор. На собственные нужды FindFace Security требуется 2 ядра. Характеристики также зависят от количества камер. Для одной камеры 1080p@25FPS требуется 2 ядра с НТ с частотой >2 ГГц.
Память	На собственные нужды FindFace Security требуется 6 Гб. Потребление памяти также зависит от количества камер. Для одной камеры 1080p@25FPS требуется 2 Гб.
Жесткий диск	На собственные нужды операционной системы и FindFace Security требуется 10 Гб. Суммарный объем определяется в зависимости от требуемой глубины архива событий в базе данных и в логе из расчета 1.5 Мб на 1 событие.
Операционная система	Только Ubuntu 16.04 x64

Примечание: Минимальная конфигурация, необходимая для обработки 1 видеопотока 720p (1280×720) 25 FPS, состоит из процессора INTEL Core i5 6-го поколения с 4-мя физическими ядрами 2,8 ГГц и 6 Гб оперативной памяти.

Совет: Для подбора требований также можно использовать результаты тестовых замеров производительности. Тестовые замеры выполнены для серверов с отдельно установленным компонентом `video-worker`, использующим для работы CPU или GPU:

- CPU i5-8400 : разрешение fullHD - 3 камеры (~33 FPS), разрешение 720 - 5 камер (33 FPS).
- GPU (1060Ti): fullHD - 10 камер (35 FPS), 720 - 15 камер (40 FPS).

1.1.3 Развертывание FindFace Security

Развертывание в ОС Ubuntu

Для вашего удобства мы предлагаем несколько вариантов развертывания FindFace Security в ОС Ubuntu:

- Развертывание из консольного инсталлятора.
- Пошаговое развертывание.
- Развертывание только компонента `video-worker` на удаленном сервере из мини-инсталлятора.

Предупреждение: Для обновления FindFace Security с предыдущей версии (1.0/ 1.1/ 1.2) используйте **только** пошаговое развертывание.

Развертывание из консольного инсталлятора

Для развертывания FindFace Security можно использовать консольный инсталлятор.

Предупреждение: Инсталлятор не предназначен для обновления FindFace Security.

Предупреждение: Для успешного функционирования системы после установки из инсталлятора, IP-адрес сервера должен быть статическим. Для того чтобы сделать IP-адрес статическим, откройте файл `etc/network/interfaces` и измените текущую запись для основного сетевого интерфейса так, как показано в примере ниже. Замените адреса в примере на актуальные с учетом настроек сети.

```
sudo vi /etc/network/interfaces

iface eth0 inet static
address 192.168.112.144
netmask 255.255.255.0
gateway 192.168.112.254
dns-nameservers 192.168.112.254
```

Перезапустите сетевые интерфейсы.

```
sudo service networking restart
```

С осторожностью редактируйте файл `etc/network/interfaces`. Перед тем как приступить к редактированию, ознакомьтесь с инструкцией по настройке сетей Ubuntu.

См.также:

- *Пошаговое развертывание*

Для развертывания из инсталлятора выполните следующие действия:

1. Загрузите файл инсталлятора `<findface-security-xxx>.run`.
2. Поместите файл `.run` в любой каталог на сервере установки (например, `/home/username`).
3. Из данного каталога сделайте файл `.run` исполняемым.

```
chmod +x <findface-security-xxx>.run
```

4. Запустите файл `.run`.

```
sudo ./<findface-security-xxx>.run
```

Инсталлятор проверит, соответствует ли сервер системным требованиям. После этого компоненты FindFace Security будут автоматически установлены, настроены и запущены в соответствии со следующей конфигурацией:

Компонент	Особенности установки
findface-postgres-facen	Устанавливается и запускается.
ffsecurity	Устанавливается и запускается.
ffsecurity-ui	Устанавливается и запускается.
videomanager-api	Устанавливается и запускается.
video-worker	Устанавливается и запускается.
findface-extraction-api	Устанавливается и запускается.
NTLS	Устанавливается и запускается.
nginx	Устанавливается и запускается.
База данных PostgreSQL	Устанавливается и запускается в стандартной конфигурации.
Сетевое хранилище Redis	Устанавливается и запускается.
Распределенное хранилище ключей ETCD	Устанавливается и запускается.
jq	Устанавливается. Используется для структурирования API-ответов от FindFace Security в формате JSON.

5. По завершении установки в консоль будет выведена информация, необходимая для использования FindFace Security:

Совет: Обязательно сохраните эти данные: они вам понадобятся.

```
#####
#           Installation is complete           #
#####
- upload your license to http://172.17.47.21:3185/
  login:          admin
  password:       OMBNics
- user interface: http://172.17.47.21/
  superuser:     admin
  password:      admin
  documentation: http://172.17.47.21/doc/
```

6. Загрузите файл лицензии через веб-интерфейс NTLS `http://<IP_адрес_сервера>:3185/#/`. Для доступа в веб-интерфейс NTLS используйте логин и пароль, выведенные в консоли.

Примечание: IP-адрес сервера в ссылках на веб-интерфейсы FindFace имеет вид 127.0.0.1 или <IP_адрес_в_сети>, в зависимости от того, принадлежит ли сервер к сети.

Важно: Не передавайте данные `superuser` (Супер Администратора) третьим лицам. Для администрирования системы создайте назначаемого администратора. Отличие назначаемого администратора от Супер Администратора в том, что последний не может лишиться прав администратора даже при смене роли.

Пошаговое развертывание

Данный раздел содержит сведения о пошаговом развертывании компонентов FindFace Security. Выполните приведенные ниже инструкции, придерживаясь заданного порядка.

Предупреждение: Перед развертыванием FindFace Security убедитесь, что корректно выставлены системное время и часовой пояс, а также включена синхронизация времени через `ntp/systemd-timesyncd`. При эксплуатации FindFace Security не допускайте резких скачков времени, чтобы исключить проблемы с работоспособностью сервисов после перезагрузки.

Совет: Предварительно ознакомьтесь с разделами *Системные требования* и *Архитектура*.

В этом разделе:

- Подготовка *deb*-пакетов к установке
- Установка необходимого стороннего ПО
- Установка сервера лицензий *NTLS*
- Установка базовой конфигурации
- Установка модуля биометрической видео-идентификации

Подготовка *deb*-пакетов к установке

Для того чтобы подготовить *deb*-пакеты FindFace Security к установке, выполните следующие действия:

1. Распакуйте пакет с компонентами.

```
sudo dpkg -i <findface-security-repo>.deb
```

2. Добавьте ключ подписи.

```
sudo apt-key add /var/findface-security-repo/public.key  
sudo apt-get update
```

3. Распакуйте пакеты с моделями нейронных сетей.

```
sudo dpkg -i findface-data*.deb
```

Установка необходимого стороннего ПО

Для работы базовой конфигурации FindFace Security необходима система управления базами данных PostgreSQL и сетевое хранилище Redis. Установите их из репозитория Ubuntu:

```
sudo apt-get update  
sudo apt install -y postgresql-server-dev-9.5 redis-server
```

Для работы модуля биометрической видео-идентификации установите распределенное хранилище ключей ETCD из распакованного пакета с компонентами FindFace Security.

```
sudo apt install -y etcd
```

Установка сервера лицензий NTLS

Вы получаете файл лицензии вместе с установочными пакетами FindFace Security. Для лицензирования в закрытой сети вам также будет предоставлен ключ аппаратной защиты Guardant.

Для того чтобы установить и настроить сервер лицензий NTLS, выполните следующие действия:

1. Установите компонент NTLS:

```
sudo apt-get update
sudo apt-get install ntls
```

Совет: В файле конфигурации NTLS вы можете изменить папку для хранения файла лицензии и настроить удаленный доступ к веб-интерфейсу NTLS, используемому для управления лицензией. Для того чтобы открыть файл конфигурации NTLS, выполните команду:

```
sudo vi /etc/ntls.cfg
```

При необходимости укажите в параметре `license-dir` другую папку для хранения файла лицензии. По умолчанию файл лицензии хранится в папке `/ntech/license`:

```
license-dir = /ntech/license
```

При необходимости раскомментируйте строку `proxy` и укажите IP-адрес прокси-сервера:

```
proxy = http://192.168.1.1:12345
```

По умолчанию доступ в веб-интерфейс NTLS возможен с любого удаленного сервера в пределах сети (`ui = 0.0.0.0:3185`). Для того чтобы обеспечить доступ к веб-интерфейсу NTLS только с определенного IP-адреса, отредактируйте параметр `ui`:

```
ui = 127.0.0.1:3185
```

2. Добавьте сервис NTLS в автозагрузку и запустите сервис:

```
sudo systemctl enable ntls && sudo systemctl start ntls
```

3. Загрузите файл лицензии в веб-интерфейсе NTLS по адресу `http://<IP-адрес NTLS>:3185/#/`.
4. В случае лицензирования в закрытой сети вставьте ключ Guardant в USB-порт.

Установка базовой конфигурации

Установка базовой конфигурации (базы данных с необходимыми расширениями, компонента `ffsecurity` и `ffsecurity-ui`) выполняется следующим образом:

1. Установите расширение `findface-postgres-9.5-facen` к PostgreSQL из пакета `<ffsecurity-repo>.deb`:

```
sudo apt install -y findface-postgres-9.5-facen
```

2. В консоли PostgreSQL создайте пользователя `ntech` и базу данных `ffsecurity`. Загрузите в базу данных расширение `findface-postgres-9.5-facen` с помощью метки `facen-compare-bytea`.

```
sudo -u postgres psql

postgres=# CREATE ROLE ntech WITH LOGIN;

postgres=# CREATE DATABASE ffsecurity WITH OWNER ntech ENCODING 'UTF-8' LC_COLLATE='en_US.UTF-
↵8' LC_CTYPE='en_US.UTF-8' TEMPLATE template0;

postgres=# \c ffsecurity;

ffsecurity=# CREATE EXTENSION "facen-compare-bytea";
```

Для выхода из консоли PostgreSQL введите \q и нажмите Enter.

3. Разрешите авторизацию в PostgreSQL по UID клиента сокета. Перезапустите PostgreSQL.

```
echo 'local all ntech peer' | sudo tee -a /etc/postgresql/9.5/main/pg_hba.conf

sudo systemctl restart postgresql@9.5-main.service
```

4. Установите компонент ffsecurity из пакета <ffsecurity-repo>.deb.

Примечание: Вместе с ffsecurity будет установлен nginx.

```
sudo apt install -y ffsecurity
```

5. Установите веб-интерфейс ffsecurity-ui из пакета <ffsecurity-repo>.deb.

```
sudo apt install -y ffsecurity-ui
```

6. Откройте файл конфигурации /etc/ffsecurity/config.py. В параметре EXTERNAL_ADDRESS укажите актуальный внешний IP-адрес или URL сервера установки, по которому будет доступен веб-интерфейс. Если компоненты videomanager-api и/или extraction-api будут установлены на удаленных серверах, укажите IP-адреса серверов в параметрах VIDEO_MANAGER_ADDRESS и/или EXTRACTION_API (установка компонентов описана в разделе см. *Установка модуля биометрической видео-идентификации*). Придумайте и укажите в параметре VIDEO_DETECTOR_TOKEN токен для авторизации распознавания лиц на видео. Данный токен будет передаваться в задачи videomanager-api.

Совет: Если необходимо обеспечить безопасность данных, включите *SSL-шифрование*.

Совет: При необходимости установите 'IGNORE_UNMATCHED': True, чтобы отключить запись события в базу данных, если обнаруженное лицо отсутствует в списках наблюдения (верификация дала отрицательный результат). Данную настройку рекомендуется использовать при большом количестве посетителей. Пороговая степень схожести при верификации лиц определяется параметром CONFIDENCE_THRESHOLD.

Совет: Рекомендуется отредактировать значение параметра MINIMUM_DOSSIER_QUALITY. Данный параметр определяет минимальное качество лица на фотографии в досье. Если качество лица хуже минимального, пользователь не сможет загрузить такую фотографию в досье. Прямые изображения лиц анфас считаются наиболее качественными. Им соответствуют значения вблизи 0, как правило, отрицательные (такие как -0.00067401276, например). Перевернутые лица и лица,

повернутые под большими углами, характеризуются отрицательным значениям от -5 и меньше. По умолчанию 'MINIMUM_DOSSIER_QUALITY': -2, что соответствует среднему качеству.

```

sudo vi /etc/ffsecurity/config.py

MEDIA_ROOT="/var/lib/ffsecurity/uploads"
STATIC_ROOT="/var/lib/ffsecurity/static"

EXTERNAL_ADDRESS="http://172.20.77.26:8000"

DEBUG = False

LANGUAGE_CODE = 'en-us'

TIME_ZONE = 'UTC'

DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.postgresql',
        'NAME': 'ffsecurity',
    }
}

# use pwgen -sncy 50 1|tr "" "." to generate your own unique key
SECRET_KEY = 'changeme'

FFSECURITY = {
    'VIDEO_DETECTOR_TOKEN': 'GOOD_TOKEN',
    'CONFIDENCE_THRESHOLD': 0.75,
    'MINIMUM_DOSSIER_QUALITY': -0.1,
    'IGNORE_UNMATCHED': False,
    'VIDEO_MANAGER_ADDRESS': 'http://127.0.0.1:18810',
    'EXTRACTION_API': 'http://127.0.0.1:18666/',
}

FFSECURITY_UI_CONFIG = {
    'plugins': {
        'genetec': True,
    },
}

```

Совет: При необходимости также отредактируйте файл конфигурации /etc/nginx/sites-available/ffsecurity-nginx.conf.

7. Используя команду `pwgen -sncy 50 1|tr "" "."`, сгенерируйте ключ подписи для шифрования сессии (используется Django) и задайте его в параметре `SECRET_KEY`.
8. Отключите сервер `nginx`, используемый по умолчанию, и добавьте в список включенных серверов сервер `ffsecurity`. Перезапустите `nginx`.

```

sudo rm /etc/nginx/sites-enabled/default

sudo ln -s /etc/nginx/sites-available/ffsecurity-nginx.conf /etc/nginx/sites-enabled/

sudo nginx -s reload

```

9. Перенесите схему базы данных из FindFace Security в PostgreSQL, создайте группы пользователей с *предустановленными правами* и первого пользователя с правами администратора (т. н. Супер Администратора).

Важно: Отличие назначаемого администратора от Супер Администратора в том, что последний не может лишиться прав администратора даже при смене роли.

```
sudo findface-security migrate

sudo findface-security create_groups

sudo findface-security createsuperuser --username admin --email root@localhost
```

10. Запустите сервисы.

Важно: Компонент `ffsecurity` включает в себя сервисы `findface-security-proto` (отвечает за HTTP и web-сокеты) и `findface-security-worker` (обеспечивает взаимодействие остальных компонентов системы). Количество экземпляров `findface-security-worker` рассчитывается по формуле $N = (\text{количество ядер CPU} - 1)$. Количество экземпляров задается после знака `@`, например, `findface-security-worker@{1,2,3}` для активации 3-х экземпляров.

```
sudo systemctl enable redis-server findface-security-proto findface-security-worker@{1,2,3,4}

sudo systemctl start redis-server findface-security-proto findface-security-worker@{1,2,3,4}
```

Установка модуля биометрической видео-идентификации

Установка модуля биометрической видео-идентификации (компонентов `videomanager-api`, `video-worker` и `extraction-api`) выполняется следующим образом:

1. Добавьте сервис ETCD в автозагрузку Ubuntu и запустите его.

```
sudo systemctl enable etcd.service && sudo systemctl start etcd.service
```

2. Установите компоненты `videomanager-api`, `video-worker` и `extraction-api`.

```
sudo apt install -y findface-videomanager-api fkvideo-worker findface-extraction-api
```

3. Откройте для редактирования файл конфигурации `/etc/findface-videomanager-api.conf`. В параметре `router_url` замените строку перед `v0/frame`, указав IP-адрес и порт компонента `ffsecurity` (задаются в параметре `EXTERNAL_ADDRESS` файла `/etc/ffsecurity/config.py`). Компонент `video-worker` будет отправлять обнаруженные лица по указанному адресу.

```
sudo vi /etc/findface-videomanager-api.conf

router_url: http://127.0.0.1:8000/v0/frame
```

4. В параметре `ntls` -> `url` укажите IP-адрес сервера лицензирования NTLS, если NTLS установлен на удаленном физическом сервере.

```
ntls:
url: http://127.0.0.1:3185/
```

5. Откройте для редактирования файл конфигурации `/etc/video-worker.ini`.

```
sudo vi /etc/video-worker.ini
```

6. В параметре `ntls-addr` укажите IP-адрес сервера лицензирования NTLS, если NTLS установлен на удаленном физическом сервере.

```
ntls-addr=127.0.0.1:3133
```

7. В параметре `mgr-static` укажите IP-адрес сервера с установленным компонентом `videomanager-api`, у которого компонент `video-worker` будет запрашивать настройки и список видеопотоков.

```
mgr-static=127.0.0.1:18811
```

8. В параметре `capacity` укажите максимальное количество видеопотоков, обрабатываемых компонентом `video-worker`.

```
capacity=10
```

9. В файле конфигурации `extraction-api` включите опцию `quality_estimator` для оценки качества лица.

Примечание: *Минимальное качество лица* на фотографии в досье задается параметром `MINIMUM_DOSSIER_QUALITY` в файле конфигурации `/etc/ffsecurity/config.py`.

```
sudo vi /etc/findface-extraction-api.ini

quality_estimator: true
```

10. В файле конфигурации `extraction-api` выключите поиск моделей для распознавания пола, возраста, эмоций и страны, передав пустые значения в параметры `gender`, `age`, `emotions` и `countries47`:

Предупреждение: Не удаляйте сами параметры, поскольку в этом случае будет выполняться поиск моделей по умолчанию.

```
models:
  gender: ''
  age: ''
  emotions: ''
  countries47: ''
```

В результате файл конфигурации `extraction-api` должен выглядеть примерно следующим образом:

```
listen: :18666
dlib:
  model: /usr/share/findface-data/normalizer.dat
  options:
    adjust_threshold: 0
    upsample_times: 1
nnd:
```

(continues on next page)

(продолжение с предыдущей страницы)

```

model: /usr/share/nnd/nnd.dat
quality_estimator: false
quality_estimator_model: /usr/share/nnd/quality_estimator_v2.dat
options:
  min_face_size: 30
  max_face_size: .inf
  scale_factor: 0.79
  p_net_thresh: 0.5
  r_net_thresh: 0.5
  o_net_thresh: 0.9
  p_net_max_results: 0
models:
  root: /usr/share/findface-data/models
  facen: elderberry_576
  gender: ''
  age: ''
  emotions: ''
  countries47: ''
  model_instances: 1
license_ntls_server: 127.0.0.1:3133
fetch:
  enabled: true
  size_limit: 10485760
max_dimension: 6000
allow_cors: false
ticker_interval: 5000

```

11. Добавьте сервисы `videomanager-api`, `video-worker`, `extraction-api` в автозагрузку Ubuntu и запустите их.

```

sudo systemctl enable findface-videomanager-api.service && sudo systemctl start findface-
↪videomanager-api.service

sudo systemctl enable video-worker.service && sudo systemctl start video-worker.service

sudo systemctl enable findface-extraction-api.service && sudo systemctl start findface-
↪extraction-api.service

```

Дополнительное развертывание `video-worker` на удаленных серверах

В случае если на удаленном сервере нужно установить только компонент `video-worker`, можно использовать мини-инсталлятор.

Для развертывания `video-worker` из мини-инсталлятора выполните следующие действия:

1. Загрузите файл инсталлятора `<video-worker-xxx>.run`.
2. Поместите файл `.run` в любой каталог на сервере установки (например, `/home/username`).
3. Из данного каталога сделайте файл `.run` исполняемым.

```
chmod +x <video-worker-xxx>.run
```

4. Запустите файл `.run`. Компонент `video-worker` будет автоматически установлен.

```
sudo ./<video-worker-xxx>.run
```

Примечание: При установке вам потребуется ответить на следующие вопросы:

- Указать IP-адрес сервера с компонентом `findface-videomanager-api`.
 - Указать, какой IP-адрес использовать для обращения к компоненту `ntls`.
 - Задать метки для привязки определенных камер к данному экземпляру `video-worker` (см. *Привязка группы камер к экземпляру `video-worker`*).
-

Совет: IP-адреса и метки могут быть заданы при запуске файла `.run` в параметрах командной строки. Используйте следующие опции: `-v`: задание IP-адреса сервера `findface-videomanager-api`, `-n`: задание IP-адреса сервера `ntls`, `-l`: задание меток для привязки определенных камер к данному экземпляру `video-worker`.

```
sudo ./<video-worker-xxx>.run -v 127.0.0.1 -n 172.163.42.34 -l "label1=true;
↳label2=true"
```

5. Откройте для редактирования файл конфигурации `/etc/video-worker.ini`.

```
sudo vi /etc/video-worker.ini
```

6. В параметре `ntls-addr` укажите IP-адрес локального сервера лицензирования NTLS.

```
ntls-addr=127.0.0.1:3133
```

7. В параметре `mgr-static` укажите IP-адрес сервера с установленным компонентом `videomanager-api`, у которого компонент `video-worker` будет запрашивать настройки и список видеопотоков.

```
mgr-static=127.0.0.1:18811
```

8. В параметре `capacity` укажите максимальное количество видеопотоков, обрабатываемых компонентом `video-worker`.

```
capacity=10
```

1.1.4 Веб-интерфейс

Работа с FindFace Security выполняется через веб-интерфейс. Для того чтобы отобразить веб-интерфейс, в адресной строке браузера введите базовый адрес веб-интерфейса и пройдите авторизацию.

Примечание: Базовый адрес задается при *установке* FindFace Security.

Важно: Для первого входа в систему после развертывания FindFace Security используйте учетную запись администратора, созданную при *установке*.

Веб-интерфейс имеет удобный и интуитивный дизайн и обеспечивает доступ к следующим функциям:

- Управление группами камер. Добавление и настройка камер. См. *Управление видеокameraми*.

- Управление списками наблюдения. Создание досье вручную и пакетно. См. *Управление базой данных досье*.
- Управление пользователями FindFace Security. См. *Управление пользователями*.
- Идентификация лиц по базе событий в режиме реального времени как на живом (видеопоток), так и на архивном (видеофайл) видео. Идентификация лиц по базе событий и досье. Сравнение 2-х лиц (см. *Руководство оператора*).

1.1.5 Управление видеокameraми

Для настройки видео-идентификации лиц добавьте камеры в FindFace Security, сгруппировав их с учетом расположения.

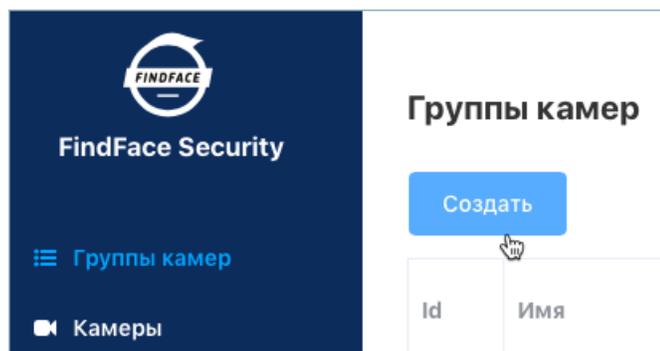
В этой главе:

- *Создание группы камер*
- *Добавление камеры в группу*
- *Мониторинг работы камер*

Создание группы камер

Для создания группы камер выполните следующие действия:

1. В веб-интерфейсе перейдите на вкладку *Группы камер*.



2. Нажмите на кнопку *Создать*.
3. Введите имя группы и при необходимости комментарий к ней.
4. Если события от камер, принадлежащих одной группе, требуется дедуплицировать, т. е. исключить одинаковые события, поставьте флажок *Дедуплицировать события* и задайте в секундах интервал дедупликации (интервал, с которым события проверяются на уникальность).
5. Поставьте флажок *Активная*.

Создать группу камер

* Имя

Комментарий

Метки

Дедуплицировать события

* Интервал дедупликации

Активная

6. Нажмите на кнопку *Сохранить*.

Добавление камеры в группу

Для добавления камеры в группу выполните следующие действия:

1. В веб-интерфейсе перейдите на вкладку *Камеры*.

Камеры

Id	Изображение

2. Нажмите на кнопку *Добавить*.

3. Введите название камеры и добавьте ее в одну из групп. При необходимости введите комментарий к камере.

Добавить камеру

* Имя

* Группа

* URL

Комментарий

Активная

4. Задайте URL камеры или адрес видеофайла для обработки.
5. Поставьте флажок *Активная*.
6. Если вы используете версию FindFace Security с обработкой видео на CPU, нажмите на кнопку *Параметры* и перейдите на вкладку *CPU*.
 - **Min face quality:** Минимальное качество изображения лица при выборе лучшего. Определяется эмпирически: отрицательные значения вблизи 0 = наиболее качественные прямые изображения лиц анфас, -1 = хорошее качество, -2 = удовлетворительное качество, отрицательные значения -5 и меньше = перевернутые лица и лица, повернутые под большими углами, распознавание может быть неэффективным.
 - **Max face angle:** Максимальное отклонение лица от положения анфас при выборе лучшего. Определяется эмпирически: -3.5 = слишком большие углы поворота, распознавание лиц может быть неэффективным, -2.5 = удовлетворительное отклонение, -0.05 = близко к положению анфас, 0 = анфас.
 - **Min face size:** Минимальный размер лица в пикселях при выборе лучшего. Чем меньше значение, тем дольше осуществляется обнаружение и отслеживание лиц. Оптимальное значение: 80-100-120. Если 0, фильтр выключен.
 - **Max face size:** Максимальный размер лица в пикселях при выборе лучшего. Если 0, фильтр выключен.
 - **Realtime mode:** Режим реального времени. Выбирать лучший кадр с лицом в каждом интервале времени `Snapshot picking interval`. Если `Post each best snapshot: true`, отправка лучшего кадра происходит по завершению каждого интервала `Snapshot picking interval`; если `false`, лучший кадр отправляется, только если его качество улучшилось по сравнению с предыдущим отправленным кадром.

- **Post each best snapshot:** Если `true`, отправлять лучший кадр в каждом интервале времени `Snapshot picking interval` в режиме реального времени. Если `false`, отправлять лучший кадр, только если его качество улучшилось по сравнению с предыдущим отправленным кадром.
- **Snapshot picking interval:** Временной интервал в миллисекундах, в течение которого в режиме реального времени выбирается лучший кадр с лицом.
- **Offline mode:** Буферный режим. Отправлять для лица один кадр наилучшего качества.
- **ROT:** Детектирование и отслеживание лиц только внутри заданной прямоугольной области. Используйте данную опцию, чтобы уменьшить нагрузку на видеодетектор лиц.
- **ROI:** Отправка в компонент `ffsecurity` только тех лиц, которые были обнаружены внутри интересующей области.

Совет: Для задания ROT/ROI удобно использовать визуальный мастер. Сначала создайте камеру без ROT/ROI, затем откройте ее для редактирования и нажмите на кнопку *Параметры*. Вы увидите визуальный мастер.

7. При необходимости задайте опциональные параметры обработки видео на CPU. Для это нажмите на кнопку *Дополнительные параметры*.

- **FFMPEG options:** Опции `ffmpeg` для видеопотока. Задаются массивом строк ключ-значение, например, `["rtsp_transport=tcp", "ss=00:20:00"]`.
- **Frame height:** Размер кадра для детектора лиц в пикселях. Отрицательные значения соответствуют исходному размеру. Оптимальные значения для уменьшения нагрузки: 640-720.
- **Tracked faces:** Максимальное количество лиц, одновременно отслеживаемых детектором лиц. Влияет на производительность.
- **Tracker threads:** Количество тредов отслеживания для детектора лиц. Должно быть меньше или равно значению параметра `persons`. Оптимально, когда они равны. Если количество тредов отслеживания меньше, чем максимальное количество отслеживаемых лиц, потребление ресурсов уменьшается, однако также уменьшается и скорость отслеживания.
- **JPEG quality:** Качество сжатия полного кадра для отправки.
- **Draw track:** Рисовать в `bbox` след от движения лица.
- **Response timeout:** Время ожидания в миллисекундах ответа на API-запрос.
- **Min motion intensity:** Минимальная интенсивность движения, которая будет регистрироваться детектором движения. Определяется эмпирически: 0 = детектор выключен, 0.002 = значение по умолчанию, 0.05 = минимальная интенсивность слишком высока, чтобы зарегистрировать движение.
- **Scale frame:** Размер кадра для детектора движения относительно исходного размера от 0 до 1. Кадр должен быть уменьшен при больших разрешениях камеры, отображении лиц крупным планом, а также при чрезмерной загрузке процессора — для снижения потребления системных ресурсов.

8. Если вы используете версию FindFace Security с обработкой видео на GPU, нажмите на кнопку *Параметры* и перейдите на вкладку *GPU*.

- **Filter min face quality:** Минимальное качество изображения лица для отправки на сервер. Определяется эмпирически: отрицательные значения вблизи 0 = наиболее качественные прямые изображения лиц анфас, -1 = хорошее качество, -2 = удовлетворительное качество,

отрицательные значения -5 и меньше = перевернутые лица и лица, повернутые под большими углами, распознавание может быть неэффективным.

- **Min face size:** Минимальный размер лица в пикселях для отправки на сервер. Если 0, фильтр выключен.
- **Max face size:** Максимальный размер лица в пикселях для отправки на сервер.
- **Min face size:** Минимальный размер лица в пикселях для отправки на сервер. Если 0, фильтр выключен.
- **JPEG quality:** Качество сжатия полного кадра для отправки.
- **FFMPEG options:** Опции ffmpeg для видеопотока. Задаются массивом строк ключ-значение, например, ["rtsp_transpotr=tcp", "ss=00:20:00"].
- **Post only the best snapshot:** Буферный режим. Отправлять для лица один кадр наилучшего качества.
- **Posting timeout:** Время ожидания в миллисекундах ответа на отправленный запрос с лицом.
- **Retrieve timestamps from stream:** Если true, отправлять на сервер временные метки из потока. Если false, отправлять текущие дату и время.
- **Add to timestamp:** Прибавлять указанное количество секунд к временным меткам из потока.

9. Нажмите на кнопку *Сохранить*.

Мониторинг работы камер

Мониторинг работы камер выполняется на вкладке *Камеры*.

The screenshot shows the 'Камеры' (Cameras) monitoring interface. At the top left, there is a 'Добавить' (Add) button. Below it is a table with the following columns: Id, Изображение (Image), Имя (Name), Группа (Group), Активная (Active), Статус (Status), and Состояние (State). The table contains one row with the following data: Id: 4, Image: [Camera thumbnail], Name: http://172.17.45.87/hls/openspase.m3u8, Group: 1, Active: [checked], Status: [Green dot] 2д 18ч 31м 49с / 51 / 0, State: INPROGRESS (with a 'Перезапустить' button). To the right of the table is a 'Фильтры' (Filters) sidebar with dropdown menus for 'Группы камер' (Camera groups) set to 'Не выбраны', 'Активный' (Active) set to 'Все', and 'Статус' (Status) set to 'Все'. There is also an 'Очистить' (Clear) button at the bottom of the filters.

Статусы камер:

- Зеленый: идет обработка видеопотока с камеры, проблем не обнаружено.
- Желтый: камера работает менее 30 секунд или имеют место ошибки при отправке лиц.
- Красный: камера не работает.

Для каждой камеры приводятся следующие статистические данные по обработке видеопотока: длительность обработки/количество успешно отправленных лиц/количество лиц, обработанных с ошибками.

Для перезапуска камеры нажмите на кнопку *Перезапустить* в столбце *Состояние*.

При большом количестве камер в системе используйте следующие фильтры:

- *Группа камер,*
- *Активная,*
- *Статус.*

1.1.6 Управление базой данных досье

FindFace Security позволяет создать досье на персону. Досье содержит одну или несколько фотографий персоны и классифицируется по принадлежности к тому или иному списку наблюдения, например, к черному или белому в самом простом случае. Вы можете создать несколько списков наблюдения, например, в зависимости от уровня опасности или, наоборот, статуса персоны.

Совет: Для автоматического создания большого количества досье используйте функционал пакетной загрузки фотографий.

В этой главе:

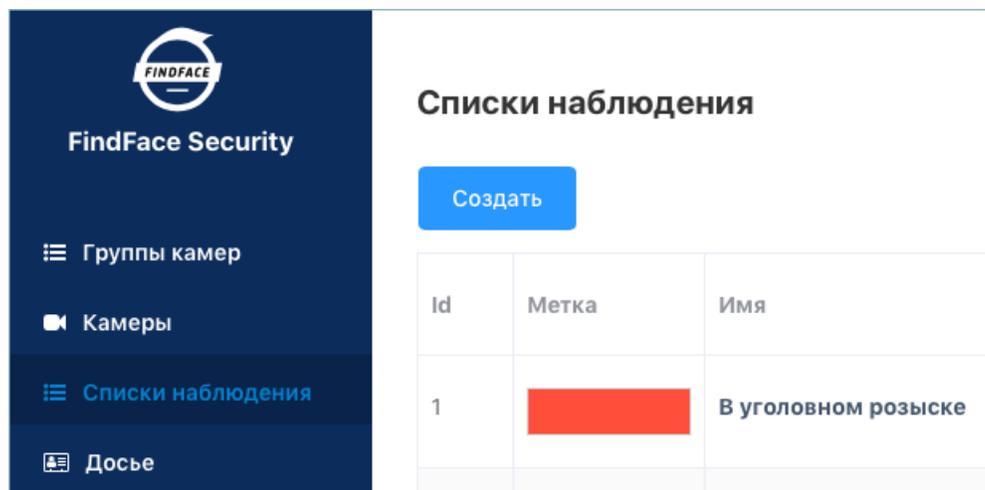
- *Списки наблюдения*
 - *Создание списка*
 - *Деактивация или удаление списка*
 - *Просмотр досье из списка*
- *Создание досье вручную*
- *Пакетная загрузка фотографий*

Списки наблюдения

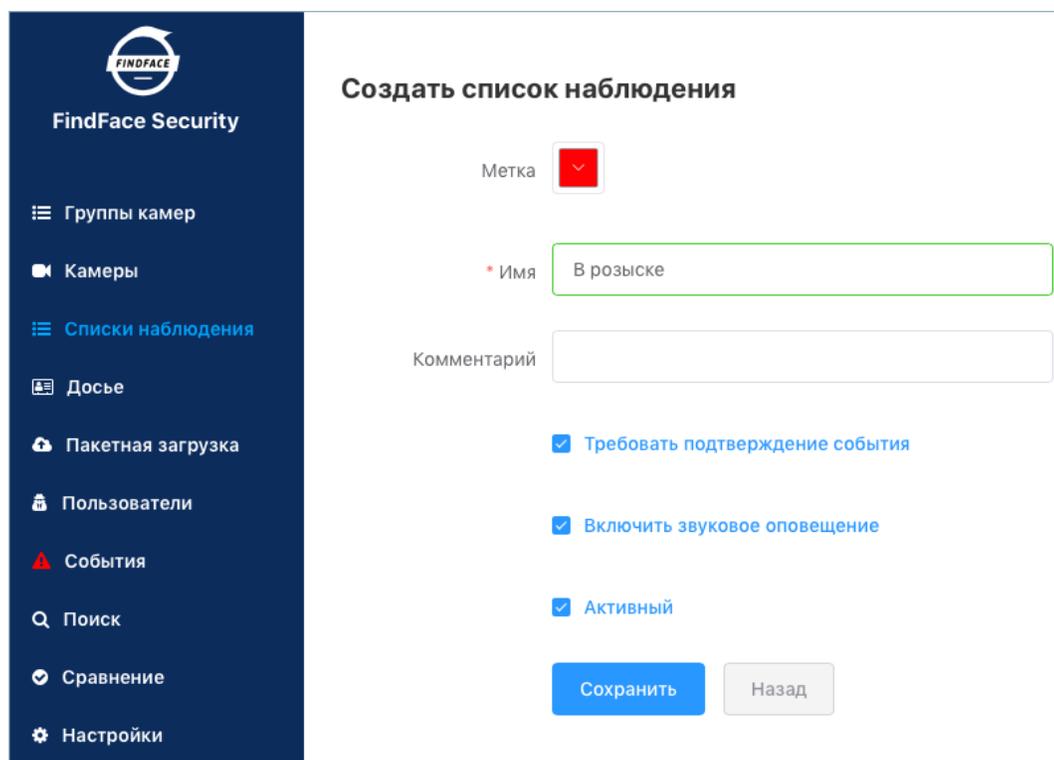
Создание списка

Для создания списка наблюдения выполните следующие действия:

1. В веб-интерфейсе перейдите на вкладку *Списки наблюдения*.



2. Нажмите на кнопку *Создать*.
3. В палитре *Метка* выберите цвет, который будет использоваться в событиях распознавания персон из данного списка. Правильно выбранный цвет повышает быстроту реагирования оператора на событие.



4. Введите название списка.
5. Поставьте флажок *Требовать подтверждение*, если для данного списка оператор должен в обязательном порядке подтвердить принятие события.
6. При необходимости включите звук при появлении события для данного списка.

7. Поставьте флажок *Активный*.
8. Нажмите на кнопку *Сохранить*.

Деактивация или удаление списка

Для того чтобы деактивировать или удалить список наблюдения из FindFace Security, выполните следующие действия:

1. Щелкните по имени списка в таблице.
2. Для деактивации снимите флажок *Активный*. Нажмите на кнопку *Сохранить*.
3. Для удаления нажмите на кнопку *Удалить*.

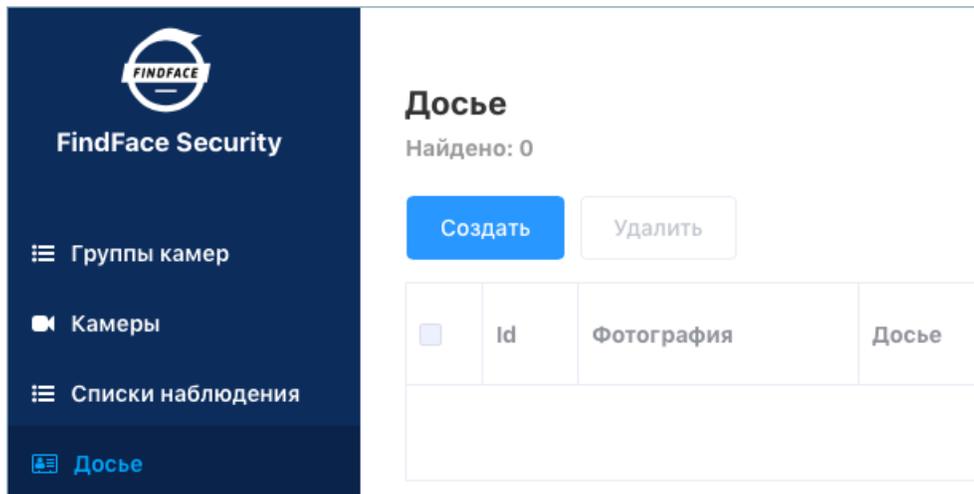
Просмотр досье из списка

Все созданные в FindFace Security досье отображаются на вкладке *Досье*. Используйте фильтр *Списки наблюдения*, чтобы отфильтровать досье по спискам.

Создание досье вручную

Для создания досье выполните следующие действия:

1. В веб-интерфейсе перейдите на вкладку *Досье*.



2. Нажмите на кнопку *Создать*.
3. Добавьте одну или несколько фотографий и введите имя человека. При необходимости добавьте комментарий.

Важно: Лицо на фотографии должно быть надлежащего качества, т. е. в близком к анфас положении. При несоответствии фотографии данному требованию будет выведено сообщение с описанием ошибки.

4. Из раскрывающегося списка *Списки наблюдения* выберите список (или несколько списков, по очереди), в который следует добавить досье.
5. Убедитесь, что поставлен флажок *Активное*. Если досье неактивно, оно не будет использоваться для *идентификации лица* в режиме реального времени.
6. Нажмите на кнопку *Сохранить*.

Пакетная загрузка фотографий

Для автоматического создания большого количества досье используйте функционал пакетной загрузки фотографий. Выполните следующие действия:

1. В веб-интерфейсе перейдите на вкладку *Пакетная загрузка*.

Пакетная загрузка досье

Журналы

Выбрать файлы или Выбрать директорию

Использовать имя файла как имя

Префикс имени

Постфикс имени

Использовать имя файла как комментарий

Префикс комментария

Постфикс комментария

* Списки наблюдения

Параллельная загрузка 2 5 10 20

2. Выберите фотографии для загрузки пофайлово или укажите папку с фотографиями.
3. Имена файлов с фотографиями можно использовать как основу для имен и/или комментариев в создаваемых досье. Выберите нужный вариант(ы). Затем настройте правило формирования имени и/или комментария, добавив пользовательский префикс и/или постфикс к имени файла.

Совет: Во избежание слияние 3-х слов в одно, используйте символ подчеркивания или пробел в префиксе и постфиксе.

4. Из раскрывающегося списка *Списки наблюдения* выберите список (или несколько списков, по очереди), в который следует добавить создаваемые досье.
5. В параметре *Параллельная загрузка* задайте количество потоков загрузки фотографий. Чем больше потоков, тем быстрее будет завершена загрузка, однако также потребуются и большее количество ресурсов.
6. Из раскрывающегося списка *MF selector* выберите, как должна поступить система при наличии нескольких лиц на фотографии: отклонить фотографию или загрузить самое большое лицо.
7. Для запуска пакетного создания досье нажмите на кнопку *Старт*.

Важно: Для просмотра лога пакетной загрузки нажмите на кнопку *Лог*. Затем при необходимости можно скачать лог в формате `.csv`.

Журналы пакетной загрузки						
Назад		Удалить		« < Страница 1 > »		
<input type="checkbox"/>	Id	Имя	Создано	Количество успешных	Количество ошибок	Скачать csv
Нет данных						
				« < Страница 1 > »		

1.1.7 Управление пользователями

Управление пользователями FindFace Security выполняется через веб-интерфейс системы на вкладке *Пользователи*.

В этой главе:

- *Роли*
- *Создание пользователя*
- *Деактивация или удаление пользователя*

Роли

Для работы с FindFace Security предусмотрены следующие роли:

- Администратор. Обладает полными правами на *управление видеокамерами, базой данных досье, событий, пользователями FindFace Security*.

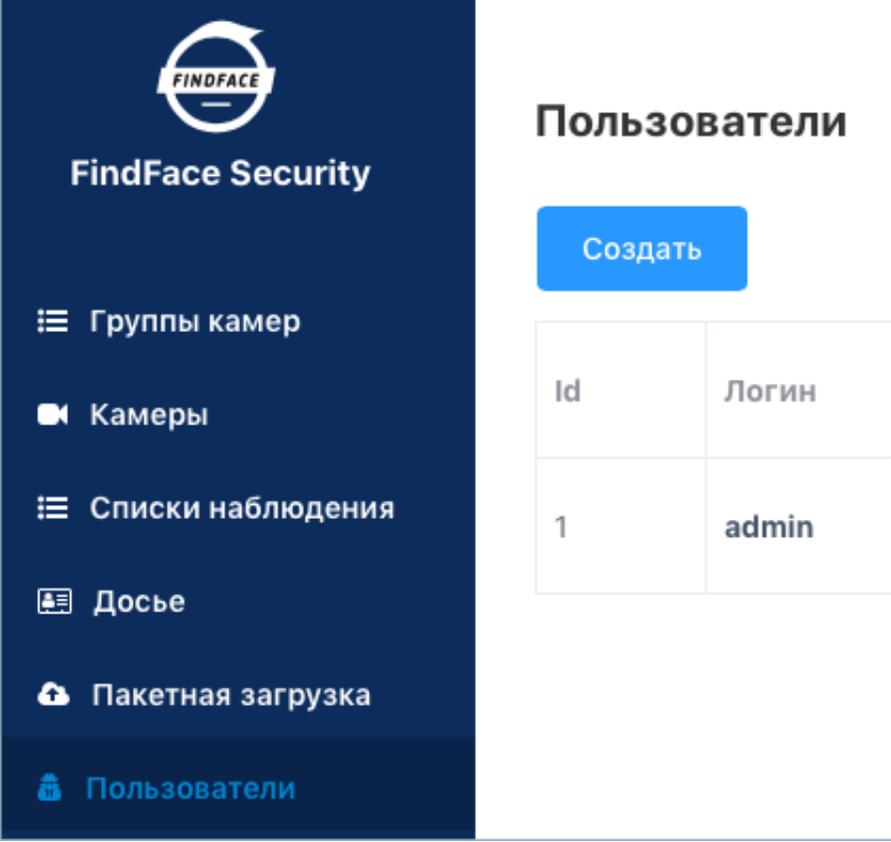
Важно: Первый *созданный при установке* администратор (Супер Администратор) не может лишиться прав даже при смене роли.

- Оператор. Обладает правами на *создание досье вручную*, подтверждение событий и поиск лиц в базах событий и досье. Остальная информация доступна в режиме чтения. *Пакетное* создание досье невозможно.
- Пользователь. Обладает правами только на подтверждение событий и поиск лиц в базе событий и досье. Остальная информация доступна в режиме чтения.

Создание пользователя

Для создания нового пользователя выполните следующие действия:

1. Нажмите на кнопку *Создать*.



The screenshot displays the 'Пользователи' (Users) management interface. On the left is a dark blue sidebar with the 'FindFace Security' logo and navigation menu items: 'Группы камер', 'Камеры', 'Списки наблюдения', 'Досье', 'Пакетная загрузка', and 'Пользователи' (highlighted). The main content area is white and titled 'Пользователи'. It features a blue 'Создать' button and a table with the following data:

Id	Логин
1	admin

2. Введите такие данные пользователя, как имя, логин и пароль, и из раскрывающегося списка *Роль* выберите одну из 3-х возможных ролей. При желании добавьте комментарий.

Создать пользователя

* Имя

* Логин

* Пароль

* Подтверждение пароля

* Роль

Комментарий

Активный

3. Поставьте флажок *Активный*.
4. Нажмите на кнопку *Создать*.

Деактивация или удаление пользователя

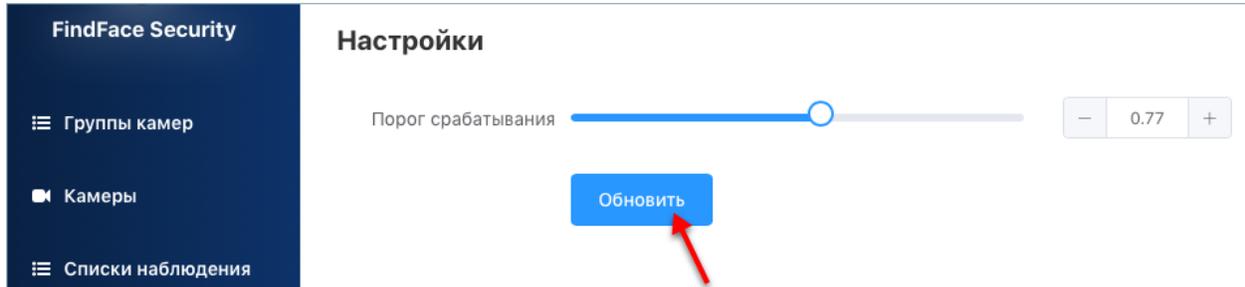
Для того чтобы деактивировать или удалить пользователя из FindFace Security, выполните следующие действия:

1. Щелкните по логину пользователя в списке.
2. Для деактивации снимите флажок *Активный*. Нажмите на кнопку *Обновить*.
3. Для удаления нажмите на кнопку *Удалить*.

1.1.8 Настройка порога верификации

FindFace Security принимает решение о совпадении (положительной верификации) обнаруженного лица с лицом из досье на основании предустановленной пороговой степени схожести. По умолчанию установлено оптимальное пороговое значение, равное 0.75. При необходимости вы можете изменить данное значение на вкладке *Настройки*.

Примечание: Чем выше пороговая степень схожести, тем меньше шансов на положительную ложную верификацию человека, однако некоторые подходящие фотографии могут также не пройти верификацию.



1.1.9 Расширенный функционал

Примечание: На данный момент расширенный функционал поддерживается только в ОС Ubuntu.

Привязка группы камер к экземпляру video-worker

Часто в распределенной архитектуре (например, сеть гостиниц, магазинов, несколько проходных) обработку видеозображения с группы камер требуется выполнять локально, не обращаясь к центральному серверу и не перераспределяя видеопотоки между удаленными экземплярами `video-worker`. В этом случае группу камер привязывают к локально установленному экземпляру.

Для обработки видео с группы камер в определенном экземпляре компонента `video-worker` выполните следующие действия:

1. В веб-интерфейсе перейдите на вкладку *Группы камер*.
2. Откройте настройки группы камер.
3. В поле *Метки* создайте или выберите из уже созданных одну или несколько меток для привязки группы камер к экземпляру `video-worker`. Сохраните изменения.
4. Откройте файл конфигурации экземпляра `video-worker` и укажите в нем заданные метки в формате `имя_метки=true` (`terminal_1` в примере ниже).

```
sudo vi /etc/video-worker.ini

wrk-labels=terminal_1=true
```

5. Перезапустите `video-worker`.

```
sudo systemctl restart video-worker.service
```

Примечание: Если камере присвоена метка, то видеопоток с нее может обрабатываться как экземпляром `video-worker` с аналогичной меткой, так и экземпляром `video-worker` без меток.

Предупреждение: Если камера с меткой обрабатывается экземпляром `video-worker` без меток и появляется свободный экземпляр с меткой, камера автоматически на него не переключится. Чтобы переключить камеру, перезапустите экземпляр `video-worker` с меткой.

Пакетная загрузка фотографий через консоль

Помимо веб-интерфейса, для пакетной загрузки фотографий в базу данных досье можно использовать поставляемую вместе с FindFace Security утилиту `findface-security-uploader`. Используйте утилиту, когда требуется загрузить большое количество фотографий (более 10000).

Выполните следующие действия:

1. Подготовьте CSV- или TSV-файл со списком фотографий и метаданными.

Важно: В качестве источника метаданных файл должен иметь следующий формат: путь к фотографии | метаданные.

Для подготовки TSV-файла можно использовать скрипт, аналогичный данному или команду `find`.

Примечание: Как скрипт, так и команда в примерах создают файл `images.tsv` с данными в формате полный путь к файлу с фотографией | метаданные. В качестве метаданных будет создана строка с именем файла.

Для запуска скрипта на создание TSV-файла со списком фотографий из указанного каталога (`/home/user/25_celeb/` в примере) выполните следующую команду:

```
python3 tsv_builder.py /home/user/25_celeb/
```

Пример использования команды `find`:

```
find photos/ -type f -iname '*g' | while read x; do y="{x%.*}"; printf "%s\t%s\n" "$x" "${y#\<br>↪#*/}"; done
```

2. Создайте файл задания (job-файл) из CSV- или TSV-файла, используя метод `add` утилиты.

```
findface-security-uploader add images.tsv
```

Опции `add`:

- `--format`: формат файла, по умолчанию `tsv`,
- `--delimiter`: используемый разделитель, по умолчанию `"\t"` для TSV-файла, `","` для формата CSV.

Примечание: Файл `job` представляет собой `sqlite`-базу, которая может быть открыта в консоли `sqlite3`.

3. Выполните задание `job`, используя метод `run` утилиты.

```
findface-security-uploader run --dossier-lists 2 --api http://127.0.0.1:80 --user admin --<br>↪password password
```

Опции run:

- `--parallel`: количество потоков загрузки фотографий, по умолчанию 10. Чем больше потоков, тем быстрее будет завершена загрузка, однако также потребуется и большее количество ресурсов.
- `--api`: URL API компонента `findface-security`, по умолчанию `http://127.0.0.1:80/`.
- `--user`: имя пользователя.
- `--password`: пароль.
- `--dossier-lists`: перечень разделенных запятой id списков наблюдения, в которые нужно добавить фотографии.
- `--failed`: в случае неудачи при обработке job-файла исправьте ошибку и повторите попытку с данной опцией.

Дедупликация событий

В этом разделе:

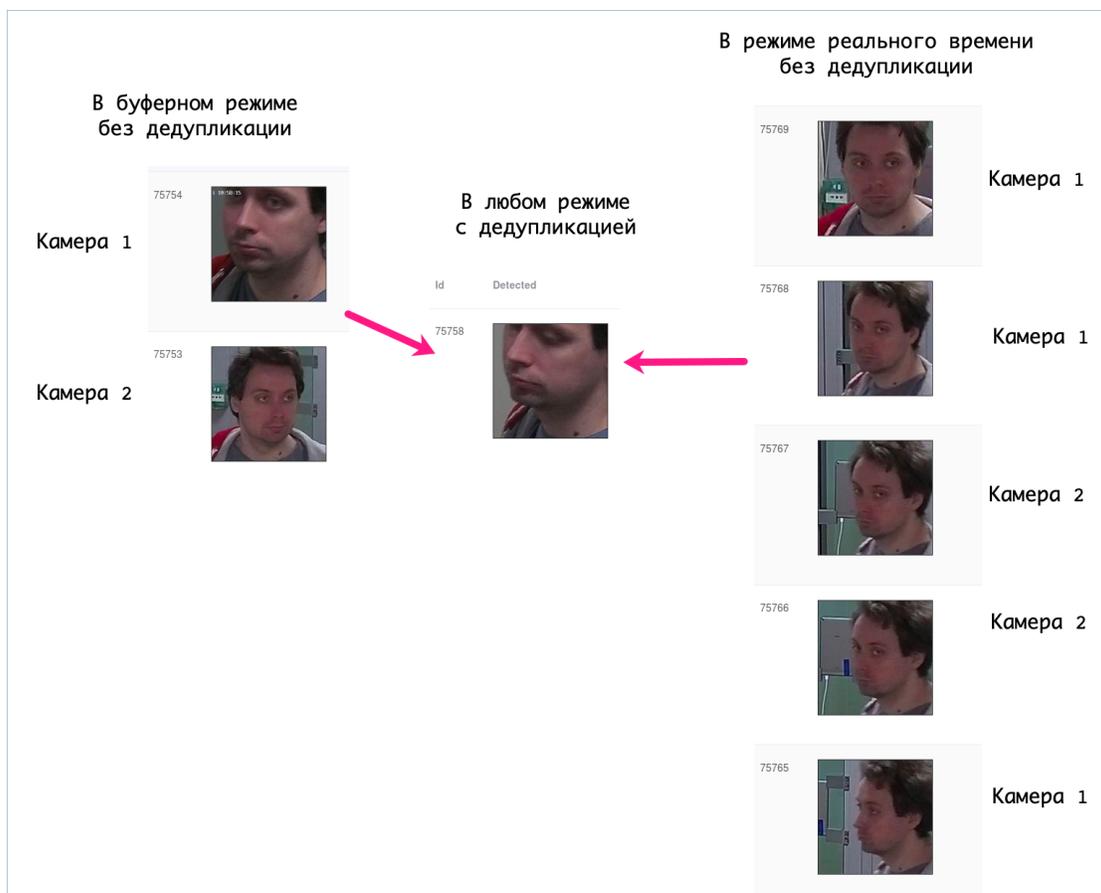
- *Алгоритм работы дедупликации*
- *Включение дедупликации*

В случае если сцены наблюдения камер, принадлежащие одной группе, приблизительно совпадают, можно использовать функцию дедупликации. Данная функция позволяет исключить регистрацию одинаковых событий в пределах группы камер.

Предупреждение: Функцию дедупликации следует использовать с крайней осторожностью, поскольку если камеры одной группы смотрят в разные стороны, возможны пропуски лиц.

Алгоритм работы дедупликации

Инфографика алгоритма дедупликации показана на схеме ниже:



1. В буферном режиме работы видеодетектора без дедупликации на сервер поступает по одному лучшему изображению лица от каждой камеры группы. Данный режим рекомендуется использовать, если камеры в группе смотрят в разные стороны.
2. В режиме реального времени без дедупликации от каждой камеры поступает несколько изображений лица. Данный режим является самым ресурсоемким с точки зрения использования дискового пространства. Также возможна чрезмерная нагрузка на сотрудников службы безопасности при большом количестве посетителей.
3. В любом режиме с дедупликацией от группы камер совокупно поступает только одно изображение лица, лучшее в текущем трекинге. Следует использовать, если сцены наблюдения камер в группе совпадают.

Включение дедупликации

Для того чтобы активировать функцию дедупликации, выполните следующие действия:

1. В веб-интерфейсе перейдите на вкладку *Группы камер*.
2. Откройте настройки группы камер.
3. Поставьте флажок *Дедуплицировать события* и задайте в секундах интервал дедупликации (интервал, с которым события проверяются на уникальность).

1.1.10 Обслуживание и устранение неисправностей

Очистка базы данных событий

Для удаления устаревших событий в ОС Ubuntu используйте утилиту `event-cleaner`.

Справка по утилите вызывается следующей командой:

```
sudo findface-security cleanup_events --help
```

```
usage: findface-security cleanup_events [-h] [--version] [-v {0,1,2,3}]
                                         [--settings SETTINGS]
                                         [--pythonpath PYTHONPATH]
                                         [--traceback] [--no-color]
                                         --age AGE

Delete old events

optional arguments:
  -h, --help            show this help message and exit
  --version             show program's version number and exit
  -v {0,1,2,3}, --verbosity {0,1,2,3}
                        Verbosity level; 0=minimal output, 1=normal output,
                        2=verbose output, 3=very verbose output
  --settings SETTINGS  The Python path to a settings module, e.g.
                        "myproject.settings.main". If this isn't provided, the
                        DJANGO_SETTINGS_MODULE environment variable will be
                        used.
  --pythonpath PYTHONPATH
                        A directory to add to the Python path, e.g.
                        "/home/djangoprojects/myproject".
  --traceback          Raise on CommandError exceptions
  --no-color           Don't colorize the command output.
  --age AGE            Minimum age in days of events to clean up
```

Для удаления событий старше определенного количества дней используйте опцию `--age`. Например, для удаления событий старше 5 дней выполните команду:

```
sudo findface-security cleanup_events --age 5
```

Для автоматического удаления событий создайте задание в планировщике `cron`. Команда в примере ниже добавляет в `cron` файл скрипта `/etc/cron.d/cleanup`, который удаляет события старше 60 дней. Скрипт выполняется ежедневно в 00:05.

```
echo '5 0 * * * root /usr/bin/findface-security cleanup_events --age 60' | sudo tee /etc/cron.d/
↳ cleanup
```

Логи

При разборе нештатных ситуаций используйте логи, содержащие подробную детализировку всех событий, произошедших в системе.

Важно: Для того чтобы включить хранение аудит-логов на жестком диске в ОС Ubuntu, в файле `/etc/systemd/journald.conf` раскомментируйте и измените параметр `Storage` следующим образом:

```
sudo vi /etc/systemd/journald.conf
...
[Journal]
Storage=persistent
```

При необходимости также раскомментируйте и измените значение параметра `SystemMaxUse`. Данный параметр определяет в процентах максимальный объем логов на жестком диске (по умолчанию 10%).

```
SystemMaxUse=15
```

Для того чтобы просмотреть аудит-логи в ОС Ubuntu, выполните следующую команду:

```
journalctl -o verbose SYSLOG_IDENTIFIER=ffsecurity
```

При расшифровке аудит-логов в первую очередь обращайтесь внимание на следующие параметры:

- `REQUEST_USER`: пользователь, который выполнил изменения;
- `REQUEST_PATH`: URL запроса;
- `REQUEST_DATA`: данные запроса.

Ниже приведен пример лога создания досье с `id=1879` пользователем `admin`.

```
Пт 2017-12-22 17:53:32.436258 MSK [s=0b5566699751426983e13241301205e9;i=e26015;
↪b=907c34cc1fde4398af63bb575587d9ba;m=246f620c449;t=560eefaf59bc5;x=ed60a136c8fc6362]
  PRIORITY=6
  _UID=123
  _GID=130
  _CAP_EFFECTIVE=0
  _BOOT_ID=907c34cc1fde4398af63bb575587d9ba
  _MACHINE_ID=a3eea61c03e041ef8e64d5c72f5fce40
  _HOSTNAME=ntechadmin
  SYSLOG_IDENTIFIER=ffsecurity
  THREAD_NAME=MainThread
  _TRANSPORT=journal
  _PID=6579
  _COMM=findface-securi
  _EXE=/opt/ffsecurity/bin/python3
  _CMDLINE=/opt/ffsecurity/bin/python /opt/ffsecurity/bin/findface-security runworker
  _SYSTEMD_CGROUP=/system.slice/system-findface\x2dsecurity\x2dworker.slice/findface-security-
↪worker@4.service
  _SYSTEMD_UNIT=findface-security-worker@4.service
  _SYSTEMD_SLICE=system-findface\x2dsecurity\x2dworker.slice
  CODE_FILE=/opt/ffsecurity/lib/python3.5/site-packages/ffsecurity/mixins.py
  CODE_LINE=94
  CODE_FUNC=finalize_response
  REQUEST_USER=admin
  LOGGER=ffsecurity.audit
  MESSAGE=N8Be05i1 POST /dossier-faces/ 201 by admin
  REQUEST_DATA={"dossier": "'1879'", "source_photo": "<InMemoryUploadedFile: 14927016033292449.
↪jpeg (image/jpeg)>"}
  REQUEST_PATH=/dossier-faces/
  REQUEST_ID=N8Be05i1
  _SOURCE_REALTIME_TIMESTAMP=1513954412436258
```

В следующем примере для досье с `id=1879` запрашивается список лиц.

```

Пр 2017-12-22 17:53:32.475467 MSK [s=0b5566699751426983e13241301205e9;i=e26016;
↪b=907c34cc1fde4398af63bb575587d9ba;m=246f6215d82;t=560eefaf634fe;x=b1374a144a46b5cd]
  PRIORITY=6
  _UID=123
  _GID=130
  _CAP_EFFECTIVE=0
  _BOOT_ID=907c34cc1fde4398af63bb575587d9ba
  _MACHINE_ID=a3eea61c03e041ef8e64d5c72f5fce40
  _HOSTNAME=ntechadmin
  SYSLOG_IDENTIFIER=ffsecurity
  THREAD_NAME=MainThread
  _TRANSPORT=journal
  _COMM=findface-securi
  _EXE=/opt/ffsecurity/bin/python3
  _CMDLINE=/opt/ffsecurity/bin/python /opt/ffsecurity/bin/findface-security runworker
  _SYSTEMD_SLICE=system-findface\x2dsecurity\x2dworker.slice
  _PID=6588
  _SYSTEMD_CGROUP=/system.slice/system-findface\x2dsecurity\x2dworker.slice/findface-security-
↪worker@2.service
  _SYSTEMD_UNIT=findface-security-worker@2.service
  CODE_FILE=/opt/ffsecurity/lib/python3.5/site-packages/ffsecurity/mixins.py
  CODE_LINE=94
  CODE_FUNC=finalize_response
  REQUEST_USER=admin
  REQUEST_DATA={}
  LOGGER=ffsecurity.audit
  MESSAGE=Dee7Qvy4 GET /dossier-faces/?dossier=1879&limit=1000 200 by admin
  REQUEST_ID=Dee7Qvy4
  REQUEST_PATH=/dossier-faces/?dossier=1879&limit=1000
  _SOURCE_REALTIME_TIMESTAMP=1513954412475467

```

Удаление экземпляра продукта

Вы можете автоматически удалить FindFace Security 1.1 вместе с базой данных с помощью скрипта `ffsec_1.1_uninstall.sh`. Перед удалением будут созданы резервные копии файлов конфигурации и базы данных.

Выполните следующие действия:

1. Загрузите скрипт `ffsec_1.1_uninstall.sh` в любой каталог на сервере установки (например, в `/home/username/`).
2. Из данного каталога сделайте скрипт исполняемым.

```
chmod +x ffsec_1.1_uninstall.sh
```

3. Запустите скрипт.

```
sudo ./ffsec_1.1_uninstall.sh
```

4. Ответьте **all** на вопрос интерактивного мастера удаления, чтобы полностью удалить FindFace Security вместе с базой данных.

1.1.11 Приложение. Настройка шифрования данных в ОС Ubuntu

Для обеспечения безопасности данных включите SSL-шифрование. Выполните следующие действия:

1. В директории с конфигурацией nginx создайте каталог для хранения информации о SSL-шифровании:

```
sudo mkdir /etc/nginx/ssl
```

2. Создайте ключ и сертификат SSL:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/nginx/ssl/my-example-  
domain.com.key -out /etc/nginx/ssl/my-example-domain.com.crt
```

Для заполнения полей сертификата вам будет предложено несколько вопросов. Ответьте на них, уделив особое внимание строке **Common Name**. В ней нужно ввести имя или публичный IP-адрес домена, связанного с сервером. Созданные файлы ключа `my-example-domain.com.key` и сертификата `my-example-domain.com.crt` будут сохранены в каталоге `/etc/nginx/ssl`.

3. Настройте nginx для использования SSL. Откройте файл конфигурации nginx. Скопируйте в него код из примера ниже.

```
sudo vi /etc/nginx/nginx.conf  
  
upstream ffsecurity {  
    server 127.0.0.1:8002;  
}  
  
# redirect from http to https version of the site  
server {  
    listen 80;  
    server_name domain.ru www.domain.ru;  
    rewrite ^(.*) https://domain.ru$1 permanent;  
    access_log off;  
}  
  
server {  
    listen 443 ssl;  
  
    ssl_certificate /etc/nginx/ssl/domain.pem;  
    ssl_certificate_key /etc/nginx/ssl/domain.key;  
  
    root /var/lib/ffsecurity;  
  
    autoindex off;  
  
    server_name domain.ru;  
  
    location @ffsec {  
        proxy_set_header Host $http_host;  
        proxy_set_header X-Forwarded-For $remote_addr;  
        proxy_set_header X-Forwarded-Proto $scheme;  
        proxy_http_version 1.1;  
        proxy_set_header Upgrade $http_upgrade;  
        proxy_set_header Connection "upgrade";  
        proxy_pass http://ffsecurity;  
    }  
  
    location /static/ {  
    }  
    location /uploads/ {  
        add_header 'Access-Control-Allow-Origin' '*';  
    }  
}
```

(continues on next page)

(продолжение с предыдущей страницы)

```

        add_header 'Access-Control-Allow-Methods' 'GET';
        add_header 'Access-Control-Allow-Headers' 'DNT,User-Agent,X-Requested-With,If-
↵Modified-Since,Cache-Control,Content-Type,Range,Authorization';
        add_header 'Access-Control-Expose-Headers' 'Content-Length,Content-Range';
        add_header 'Access-Control-Max-Age' 2592000;
    }
    location /ui-static/ {
        alias /usr/share/ffsecurity-ui/ui-static/;
    }
    location /doc/ {
        alias /opt/ffsecurity/doc/;
    }
    location / {
        try_files $uri $uri/ @ffsec;
        client_max_body_size 100m;
        alias /usr/share/ffsecurity-ui/;
    }
}

```

4. Перезапустите nginx.

```
sudo service nginx restart
```

5. Внесите изменения в файл конфигурации ffsecurity. В параметре EXTERNAL_ADDRESS измените приставку `http://` на `https://`.

```
sudo vi /etc/ffsecurity/config.py

EXTERNAL_ADDRESS="https://my-example-domain.com"
```

6. Если есть запущенные процессы `video-worker`, нужно либо пересоздать камеры в веб-интерфейсе, либо изменить значение параметра `router_url` в job-заданиях, заменив приставку `http://` на `https://`. Это можно сделать с помощью команды, аналогичной следующей:

```
curl -s localhost:18810/jobs | jq -r '.[]["id"]' | xargs -I {} curl -X PATCH -d '{"router_url
↵": "https://domain.ru/video-detector/frame"}' http://localhost:18810/job/{}

```

1.2 Руководство оператора

1.2.1 Веб-интерфейс

Работа с FindFace Security выполняется через веб-интерфейс. Для того чтобы отобразить веб-интерфейс, введите его адрес в адресной строке браузера и пройдите авторизацию.

Примечание: Логин и пароль для авторизации выдаются администратором.

Веб-интерфейс имеет удобный и интуитивный дизайн и обеспечивает доступ к следующим функциям:

- Поиск лиц в базах данных. См. *Идентификация лиц по базам данных*.
- Идентификация лиц по базам данных в режиме реального времени. См. *Идентификация лиц в режиме реального времени*.

- Сравнение 2-х лиц. См. *Сравнение лиц*.
- Работа с досье на персону. См. *Работа с досье* (только для пользователей с правами оператора).

1.2.2 Идентификация лиц по базам данных

FindFace Security позволяет выполнять идентификацию (поиск) лиц по следующим базам данных:

- База данных обнаруженных на видео лиц (вкладка *События*).
- База данных досье (вкладка *Досье*). Содержит эталонные изображения лиц.

Поиск лиц выполняется на вкладке *Поиск*.

В этой главе:

- *Идентификация лица по базе данных обнаруженных лиц*
- *Идентификация лица по базе данных досье*

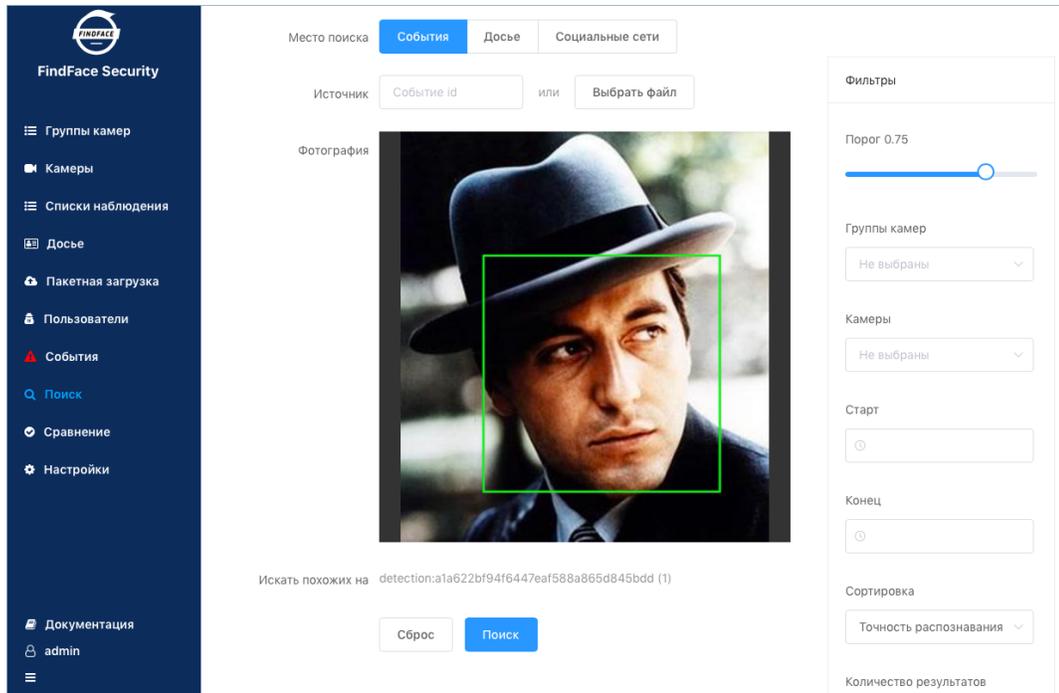
Идентификация лица по базе данных обнаруженных лиц

FindFace Security позволяет выполнять идентификацию лица по базе данных обнаруженных на видео лиц.

Примечание: В интерфейсе база данных представлена списком событий (вкладка *События*).

Для идентификации лица по базе данных выполните следующие действия:

1. Перейдите на вкладку *Поиск*.



2. Укажите место поиска: *События*.
3. Загрузите фотографию. Фотография будет отображена в одноименном поле. Если на фотографии присутствует несколько лиц, выберите нужное.

Примечание: Вместо фотографии можно указать ID события, лицо из которого нужно найти в базе данных.

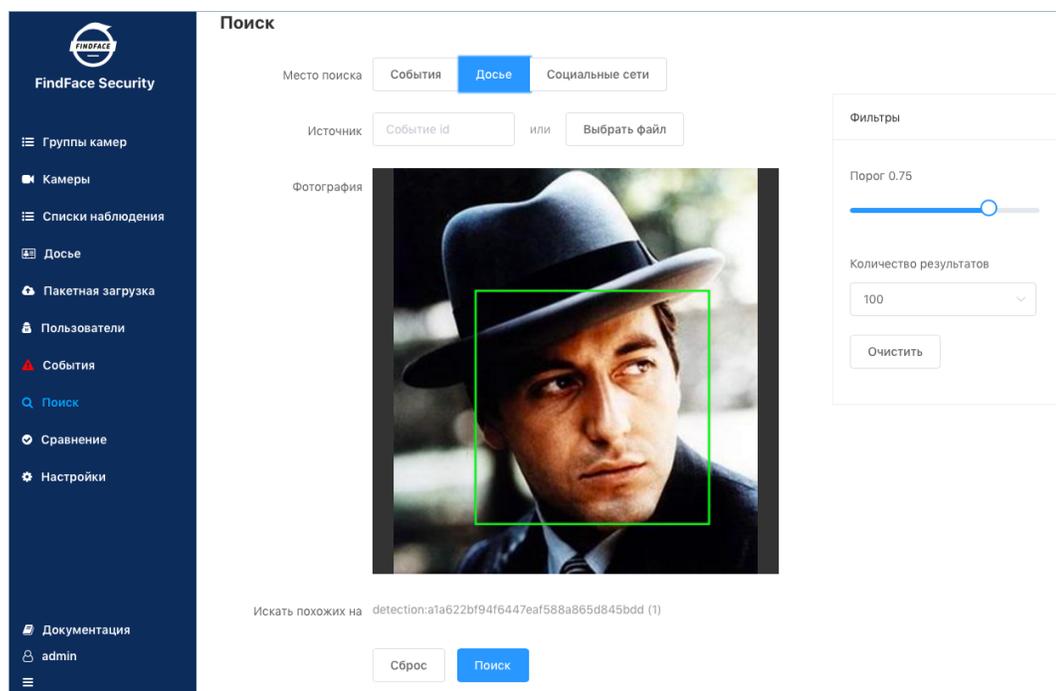
4. По умолчанию в результатах поиска отображаются лица, степень схожести которых с искомым равна или превышает 0.75. При необходимости измените данное значение.
5. При необходимости укажите группу камер и период времени, в течение которого произошло событие.
6. Результаты поиска могут быть отсортированы как в порядке уменьшения степени схожести лиц, так и по дате события (сначала самые последние события). Выберите нужную опцию в списке *Сортировка*: *Точность распознавания* или *Дата* соответственно.
7. Укажите максимальное количество событий в результатах поиска.
8. Нажмите *Поиск*. Результаты поиска будут отображены ниже. Для каждого найденного лица будет указана вероятность его совпадения с лицом на фотографии.

Идентификация лица по базе данных досье

FindFace Security позволяет выполнять идентификацию лица по базе данных, содержащей досье с эталонными изображениями лиц.

Для идентификации лица по базе данных выполните следующие действия:

1. Перейдите на вкладку *Поиск*.



2. Укажите место поиска: *Досье*.
3. Загрузите фотографию. Фотография будет отображена в одноименном поле. Если на фотографии присутствует несколько лиц, выберите нужное.

Примечание: Вместо фотографии можно указать ID события, лицо из которого нужно найти в базе данных.

4. По умолчанию в результатах поиска отображаются лица, степень схожести которых с искомым равна или превышает 0.75. При необходимости измените данное значение.
5. Укажите максимальное количество досье в результатах поиска.
6. Нажмите *Поиск*. Результаты поиска будут отображены ниже. Для каждого найденного лица будет указана вероятность его совпадения с лицом на фотографии.

1.2.3 Идентификация лиц в режиме реального времени

Мониторинг работы системы по части идентификации лиц на видеоизображении в режиме реального времени выполняется на вкладке *События*. Для идентификации в режиме реального времени может использоваться как живое (видеопоток с камеры), так и архивное (видеофайл) видео. Помимо работы с текущими событиями идентификации, данная вкладка также предоставляет доступ к истории.

Совет: Поиск лица в списке событий и базе данных досье с эталонными изображениями лиц выполняется на вкладке *Поиск*.

В этой главе:

- Просмотр событий идентификации в режиме реального времени
- Карточка события. Принятие события
- Карточка события. Поиск лица

Просмотр событий идентификации в режиме реального времени

При обнаружении лица в списке событий выводится уведомление.

Уведомление содержит следующую информацию:

- Если на лицо отсутствует досье: нормализованное изображение лица, дата и время обнаружения лица, группа камер.
- Если на лицо заведено досье: нормализованное изображение лица, фотография из досье, имя персоны, степень схожести лиц, комментарий из досье, список досье, дата и время обнаружения лица, группа камер.

Примечание: Система может быть настроена таким образом, что уведомления будут выводиться только для лиц с досье.

Важно: Для того чтобы остановить вывод новых уведомлений, нажмите на кнопку  над списком событий.

К событиям (уведомлениям) в списке можно применить следующие фильтры:

- *Досье:* отображать только события по определенному досье.
- *Списки наблюдения:* отображать только события по определенному списку наблюдения.
- *Совпадения:* отображать только события с совпадением/без совпадений или все события.
- *Подтверждено:* отображать только принятые/непринятые или все события.

- *Камеры*: отображать только события по определенной камере.
- *Группы камер*: отображать только события по определенной группе камер.
- *Старт, Конец*: отображать только события, случившиеся в определенный период времени.
- *id*: отобразить событие с определенным ID.

Карточка события. Принятие события

Для того чтобы перейти в карточку события из списка событий, щелкните в уведомлении по результату распознавания (*Нет совпадений* или имя из досье).

Карточка содержит ту же информацию, что и *уведомление*, а также предоставляет возможность принять событие. Для того чтобы это сделать, поставьте флажок *Подтверждение события*. Нажмите на кнопку *Сохранить*.

Id 15279 [События](#) [Досье](#) [Социальные сети](#)

Имя нет [+ Создать досье](#)

Точность нет
распознавания

Комментарий нет

Время 2018-09-29 23:33:28

Камера [Выход 3](#)

Группа камер [Терминал прибытия](#)

Списки наблюдения

[Подтверждение события](#)

[Сохранить](#) [Назад](#)

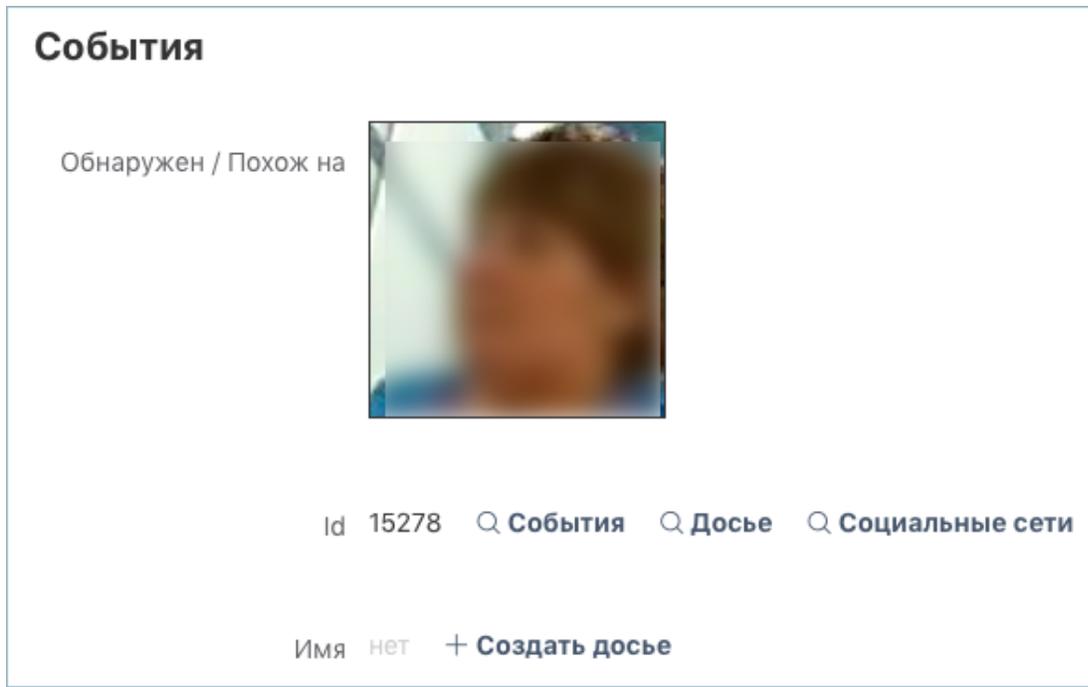
Совет: Если на обнаруженное лицо заведено досье, в него можно перейти, щелкнув по имени персоны в карточке события.

Совет: Для того чтобы принять все события, нажмите на кнопку  над списком событий.

Примечание: Принятие события может быть автоматизировано для выбранных списков наблюдения.

Карточка события. Поиск лица

FindFace Security позволяет искать обнаруженные лица в базе данных обнаруженных лиц и в базе данных досье с эталонными изображениями лиц. Для перехода на вкладку поиска из карточки события нажмите *События* и *Досье*.



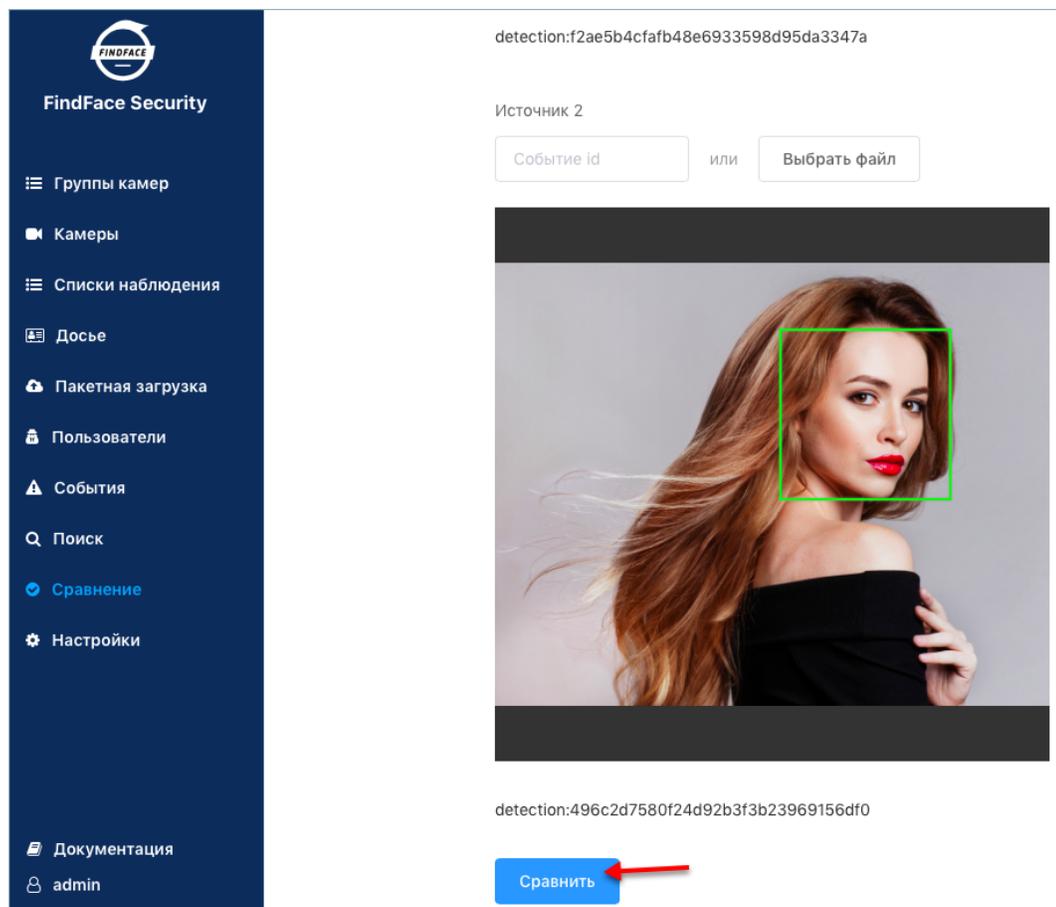
См.также:

- *Идентификация лиц по базам данных.*

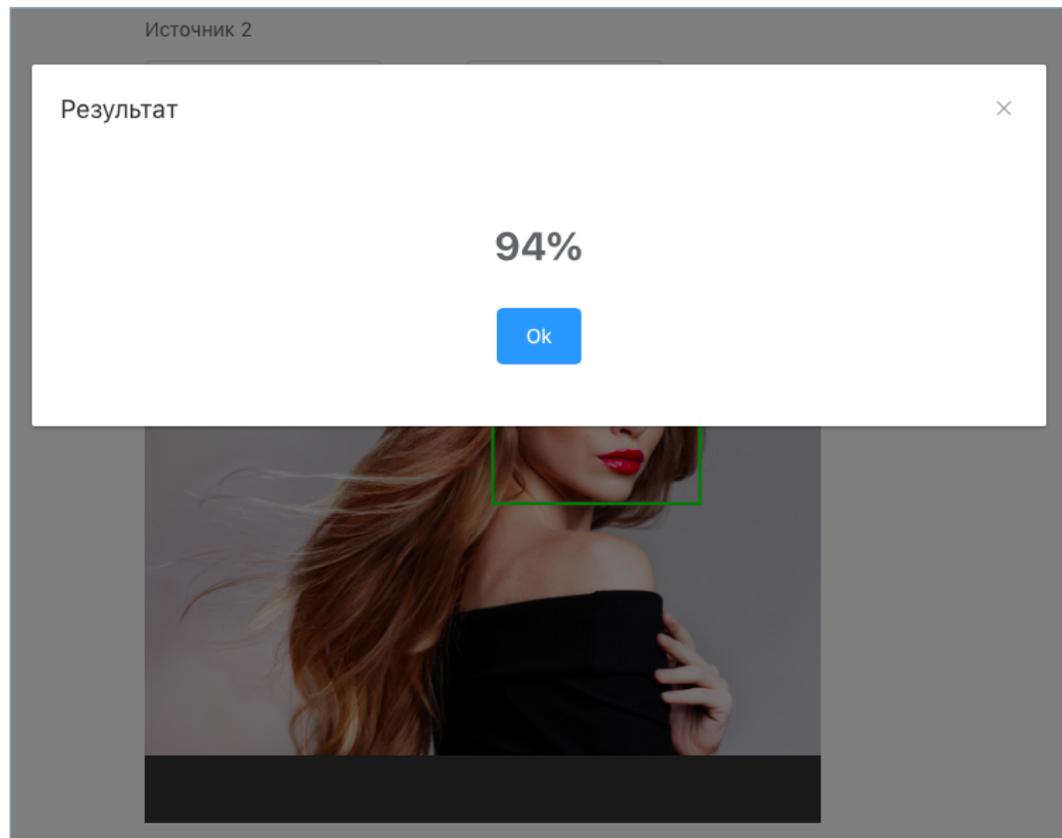
1.2.4 Сравнение лиц

FindFace Security позволяет выполнять сравнение 2-х лиц. Выполните следующие действия:

1. Перейдите на вкладку *Сравнение*.



2. Укажите id событий, лица из которых нужно сравнить, и/или загрузите фотографии с лицами.
3. Нажмите *Сравнить*. В результате будет отображена вероятность принадлежности лиц одному человеку.



1.2.5 Работа с досье

FindFace Security позволяет создавать досье на интересующих лиц, содержащее одну или несколько фотографий. Досье классифицируется по принадлежности к тому или иному списку наблюдения.

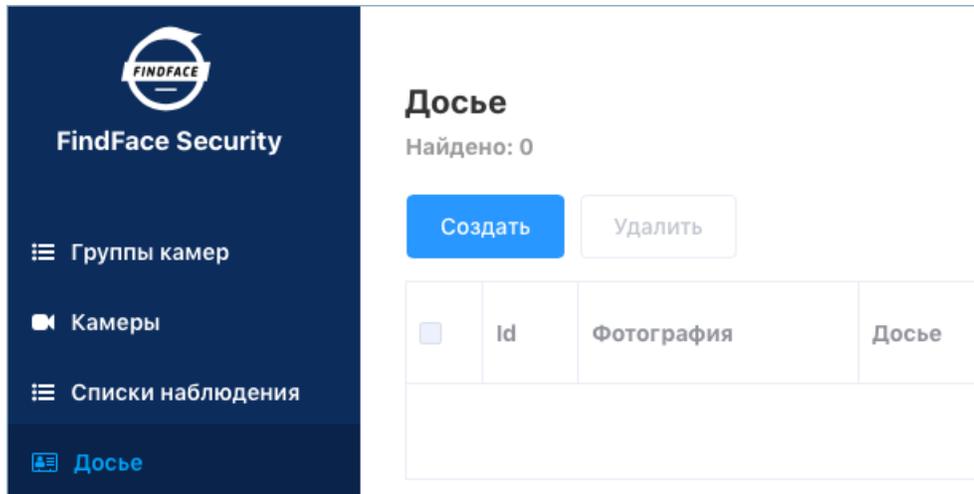
В этой главе:

- *Создание досье*
- *Просмотр досье из списка наблюдения*

Создание досье

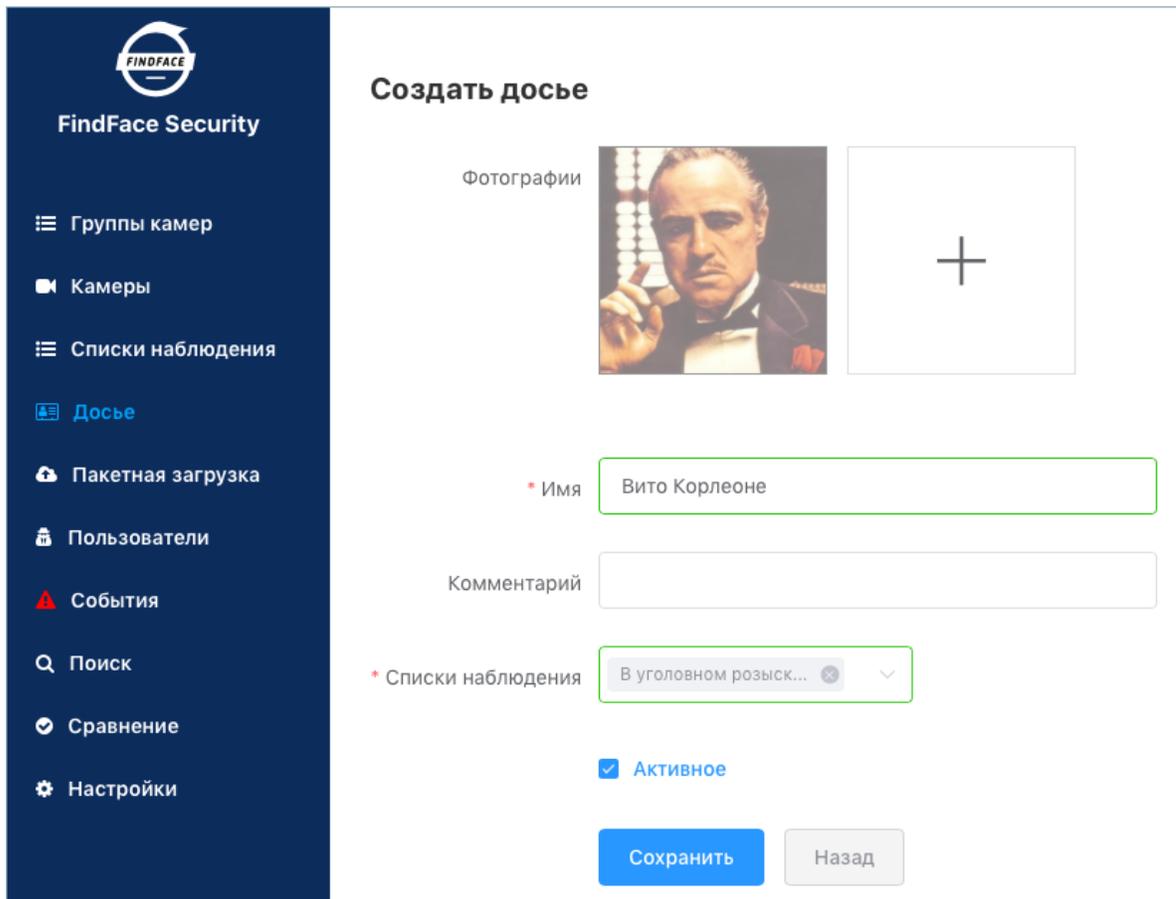
Для создания досье выполните следующие действия:

1. В веб-интерфейсе перейдите на вкладку *Досье*.



2. Нажмите на кнопку *Создать*.
3. Добавьте одну или несколько фотографий и введите имя человека. При необходимости добавьте комментарий.

Важно: Лицо на фотографии должно быть надлежащего качества, т. е. в близком к анфас положении. При несоответствии фотографии данному требованию будет выведено сообщение с описанием ошибки.



4. Из раскрывающегося списка *Списки наблюдения* выберите список (или несколько списков, по очереди), в который следует добавить досье.
5. Убедитесь, что поставлен флажок *Активное*. Если досье неактивно, оно не будет использоваться для *идентификации лица* в режиме реального времени.
6. Нажмите на кнопку *Сохранить*.

Просмотр досье из списка наблюдения

Все созданные в FindFace Security досье отображаются на вкладке *Досье*. Используйте фильтр *Списки наблюдения*, чтобы отфильтровать досье по спискам.

1.2.6 Мобильный веб-интерфейс

Для работы с FindFace Security также можно использовать упрощенную мобильную версию системы. Мобильное приложение FindFace Security поставляется по запросу для Android.

В приложении введите свой логин и пароль FindFace Security, а также адрес сервера FindFace Security и пройдите авторизацию.

16:43

FindFace Security

Login
admin

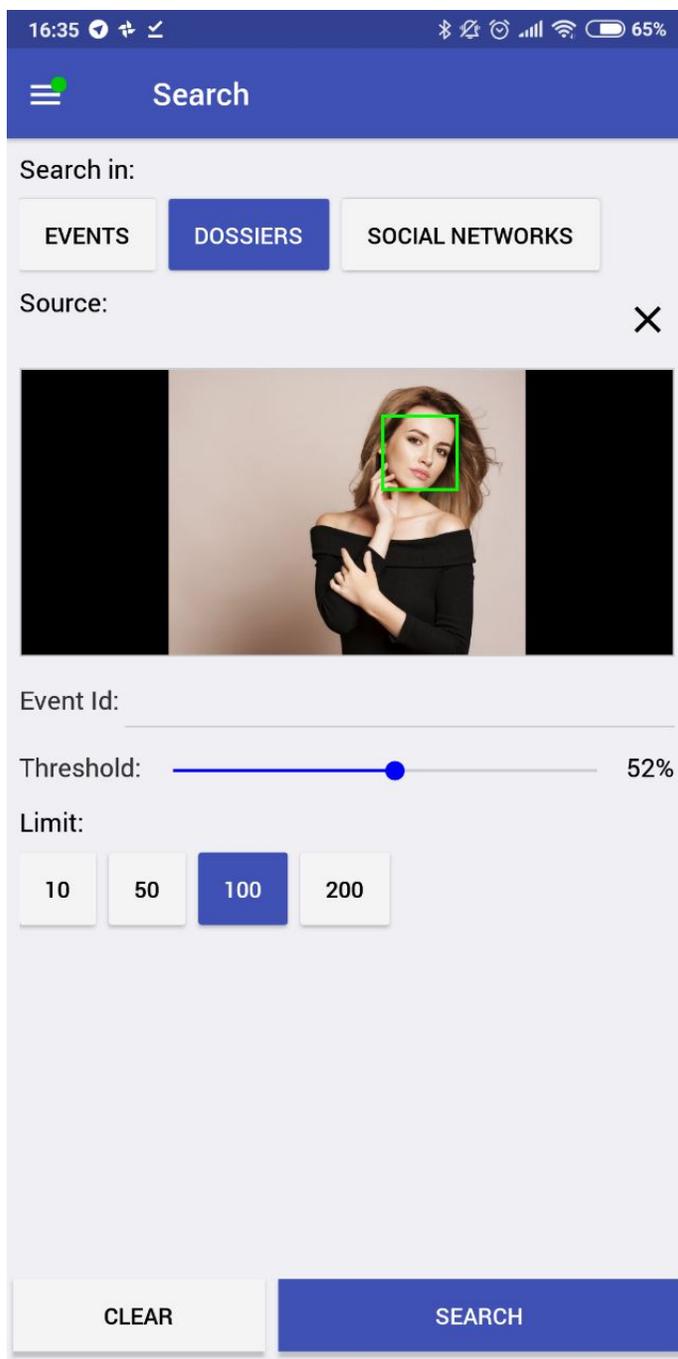
Password
.....

Url
http://172.20.77.58

LOGIN

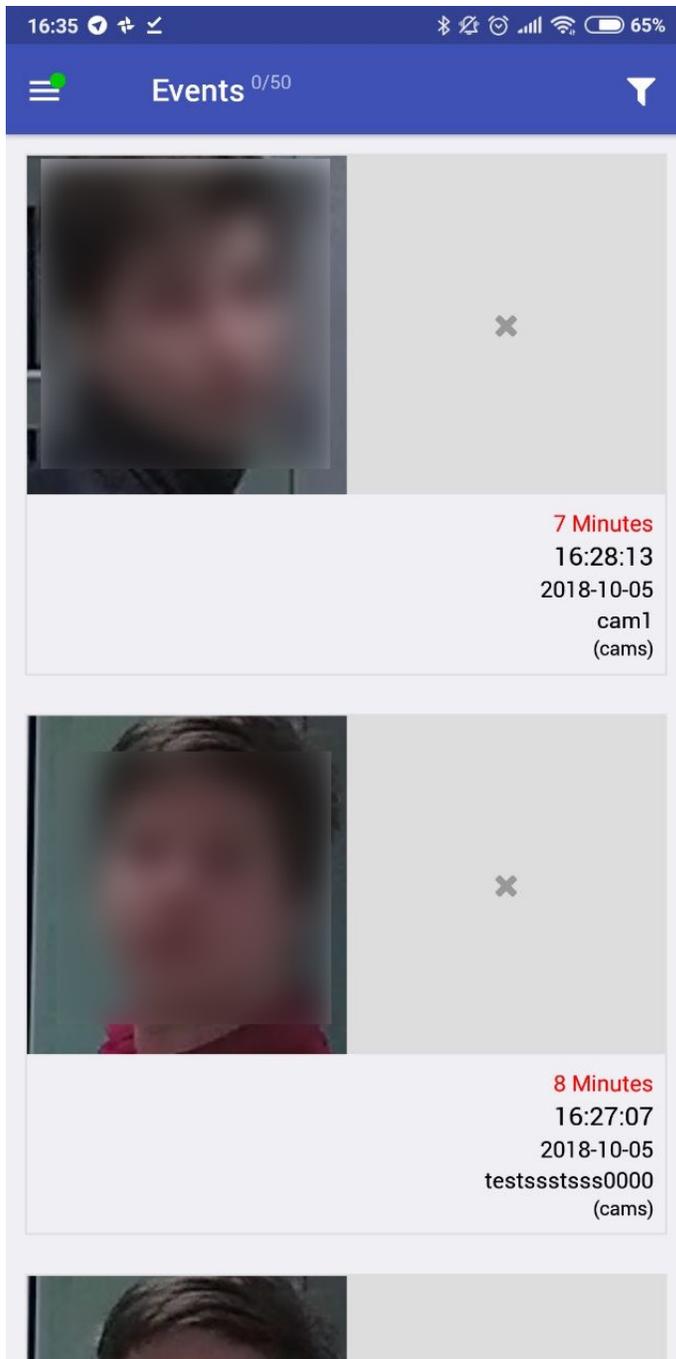
Мобильный веб-интерфейс имеет удобный и интуитивный дизайн и обеспечивает доступ к следующим функциям:

- Поиск лиц в базах данных.

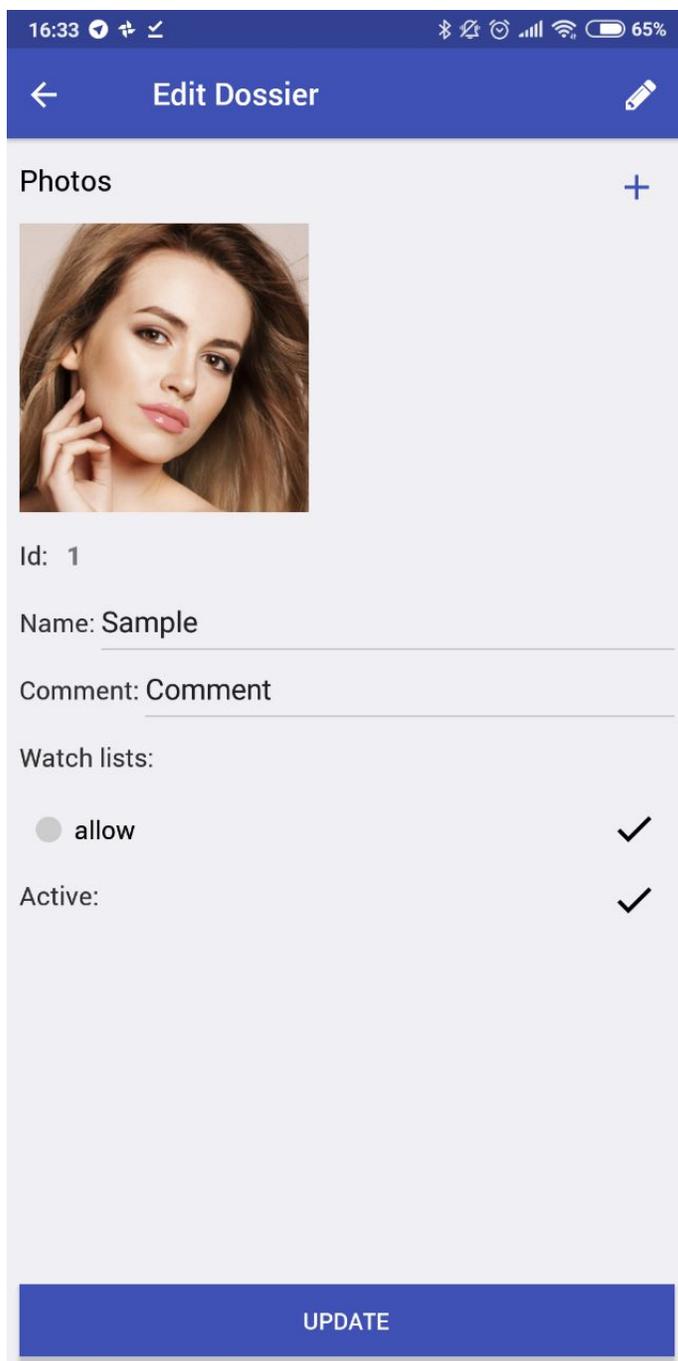


- Идентификация лиц по базам данных в режиме реального времени.

Важно: Для того чтобы в мобильной версии получать события в формате push-оповещений, для соответствующего списка наблюдения нужно поставить флажки *Требовать подтверждение события* и *Включить звуковое оповещение* (через полноформатный веб-интерфейс).



- Работа с досье на персону.



Работа с данными функциями аналогична полноформатной версии.

1.3 Интеграция с партнерами

1.3.1 Genetec Security Center

Интеграция FindFace Security с программным комплексом Genetec Security Center позволяет добавлять функционал распознавания лиц в системы безопасности на базе Genetec.

Настройка интеграции

Интеграция с Genetec Security Center реализуется через плагин `findface-genetec`. По умолчанию плагин активен и на панели навигации FindFace Security есть вкладка *Genetec*.

Примечание: Если это не так в FindFace Security, откройте файл конфигурации `ffsecurity` и проверьте, есть ли в нем активная строка `INSTALLED_APPS.append('ffsecurity_genetec')`.

```
sudo vi /etc/ffsecurity/config.py

...

FFSECURITY_UI_CONFIG = {
}

# integration plugins
INSTALLED_APPS.append('ffsecurity_genetec') # remove or comment out this line to disable
```

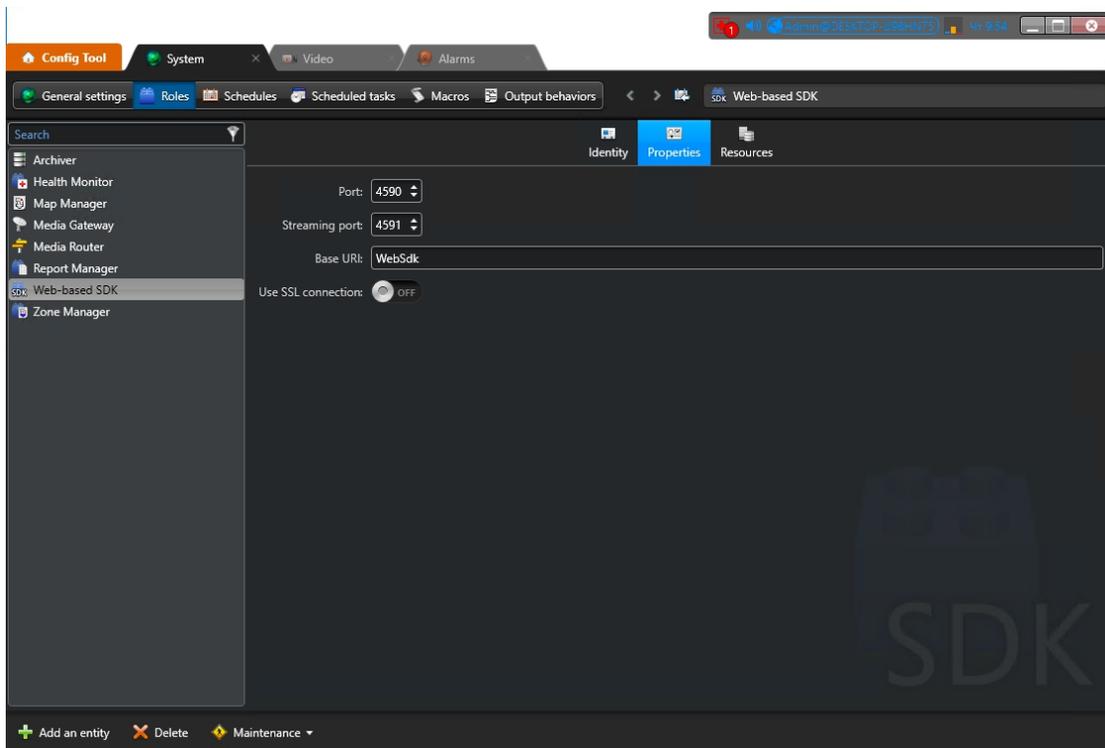
Перед настройкой интеграции на стороне FindFace Security разверните программное обеспечение Genetec Web SDK и Media Gateway и создайте в Genetec Security Center оповещение **Alarm**, которое будет отображаться при наступлении в FindFace Security события распознавания лица.

В этой главе:

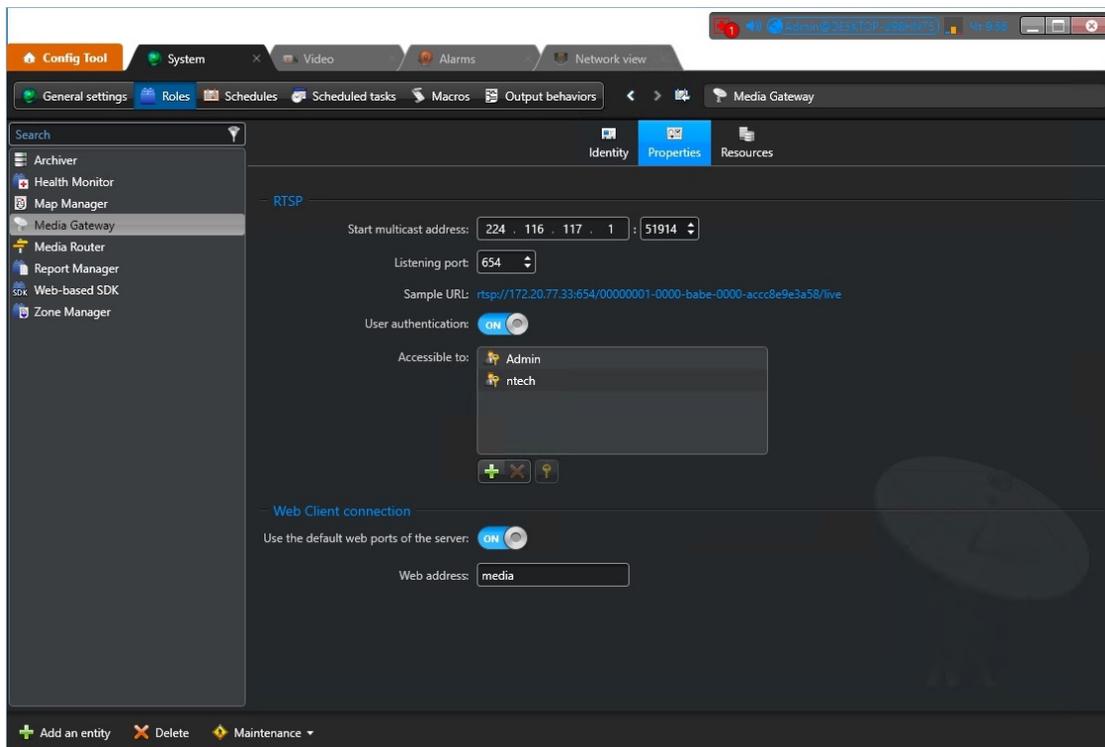
- *Настройка Genetec Web SDK и Media Gateway*
- *Создание оповещения в Genetec Security Center*
- *Настройка точек доступа в FindFace Security*
- *Импорт камер из Genetec Security Center*
- *Создание списков наблюдения и досье в FindFace Security*

Настройка Genetec Web SDK и Media Gateway

Для того чтобы развернуть Web SDK, используйте ПО Genetec Config Tool. Детали настройки приведены в официальной справочной документации *Security Center Administrator Guide -> Chapter 52: Role Types -> Web-based SDK configuration tabs*.



Для того чтобы развернуть Media Gateway в Genetec Config Tool, ознакомьтесь с содержанием главы *Security Center Administrator Guide -> Chapter 24: Video Deployment*.

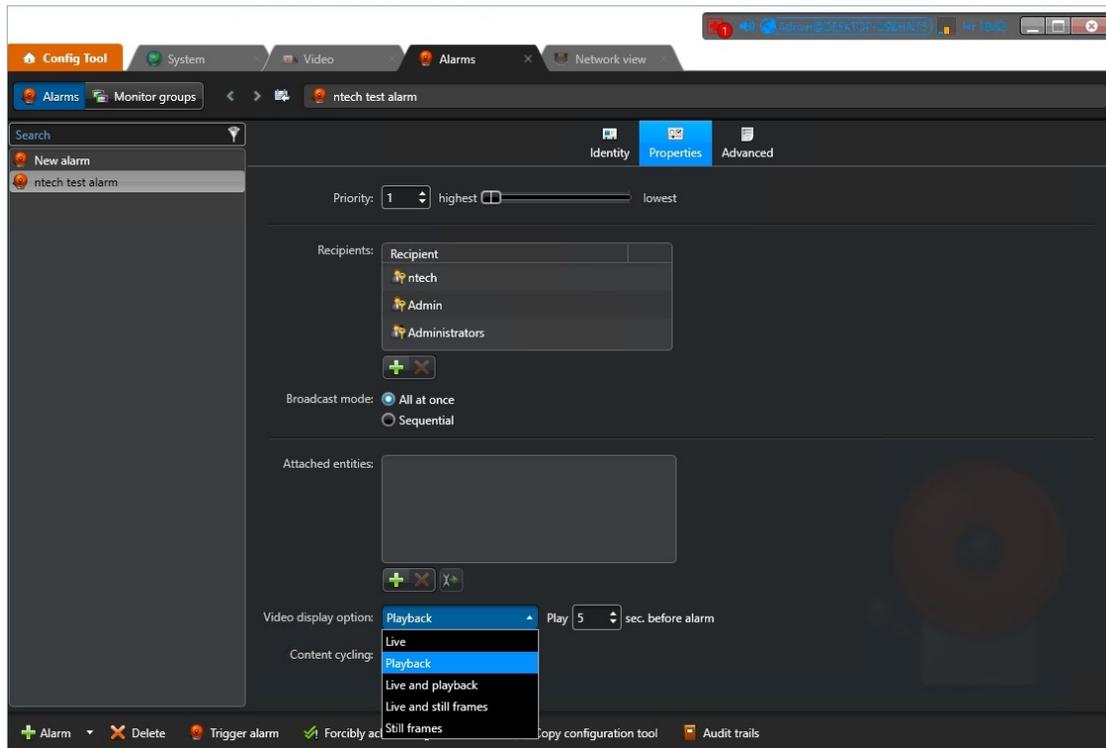


Важно: Убедитесь, что фаервол настроен таким образом, что порты WebSDK и Media Gateway

остаются открытыми.

Создание оповещения в Genetec Security Center

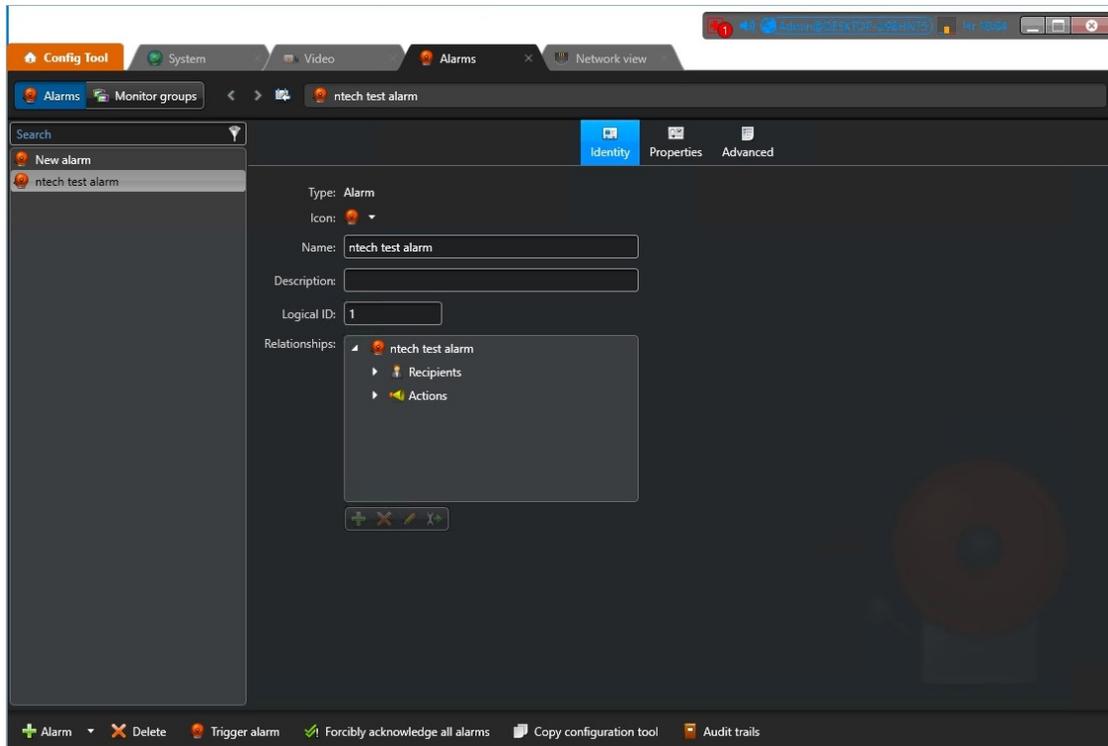
Создайте и настройте новое оповещение Alarm в Genetec Config Tool, руководствуясь разделом *Security Center Administrator Guide -> Chapter 48: Alarms -> Creating Alarms* документации.



Совет: На вкладке *Properties* выберите ту опцию отображения видео *Video display option*, которая в наибольшей степени соответствует вашим нуждам. Доступные опции *Live*, *Playback*, и т. д.

Совет: Для того чтобы активировать операции с оповещением Alarm Procedures и автоповорот видео непосредственно во всплывающем окне оповещения, включите *Content cycling*.

При настройке интеграции на стороне FindFace Security вам потребуется ввести логическое id оповещения, которое задается на вкладке *Identity*.



Настройка точек доступа в FindFace Security

Для того чтобы установить соединение между FindFace Security и Genetec Security Center, выполните следующие действия:

1. Перейдите на вкладке *Genetec* в FindFace Security.

Настройки genetec Русский

Состояние: Сконфигурирован

[Конфигурация](#) Камеры

Сервер

Host:

Port:

Пользователь:

Пароль:

Base uri:

Media

Media host:

Media port:

Пользователь:

Пароль:

Ids

Alarm id:

Application id:

[Сохранить](#)

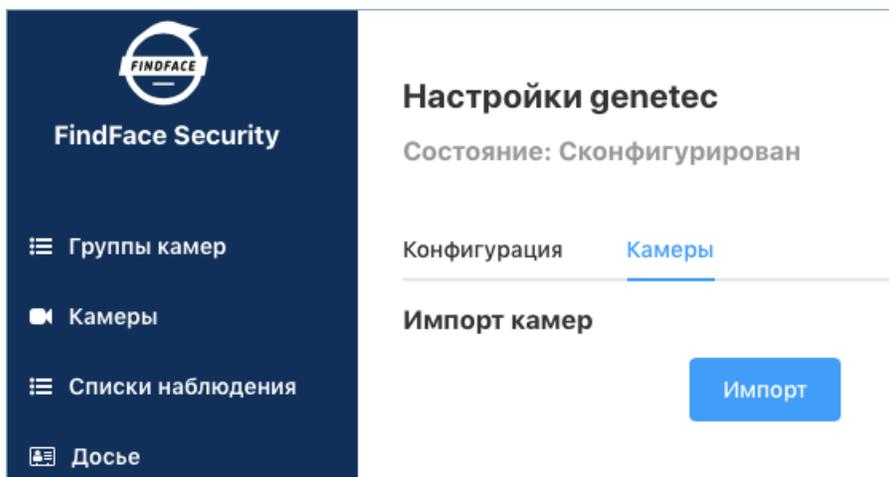
- В секциях *Сервер* и *Media*, укажите *настройки* точек доступа Web SDK и Media Gateway.

Важно: Порты WebSDK и Media Gateway должны быть открыты.

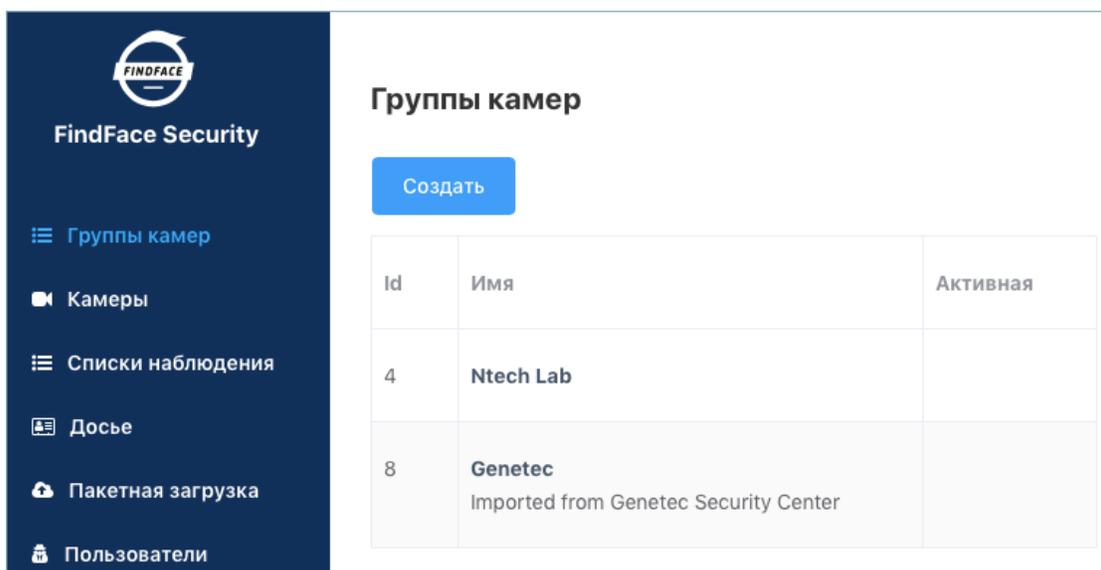
- В секции *Ids*, укажите *логический id* оповещения **Alarm**, которое будет отображаться в Genetec Security Center при наступлении события распознавания лица в FindFace Security.
- Нажмите *Сохранить*. Если соединение с Genetec Security Center успешно установлено, статус *State* будет автоматически изменен на *Сконфигурирован*.

Импорт камер из Genetec Security Center

Как только соединение с Genetec Security Center установлено, можно импортировать камеры. Для этого выберите *Камеры* на вкладке *Genetec* и нажмите *Импорт*.



Данное действие создаст *группу камер Genetec*, включающую в себя все камеры из Genetec Security Center.



Для того чтобы посмотреть список камер, на панели навигации FindFace Security перейдите на вкладку *Камеры*. Для того чтобы исключить камеру из распознавания лиц, просто деактивируйте ее в этом списке.

Создание списков наблюдения и досье в FindFace Security

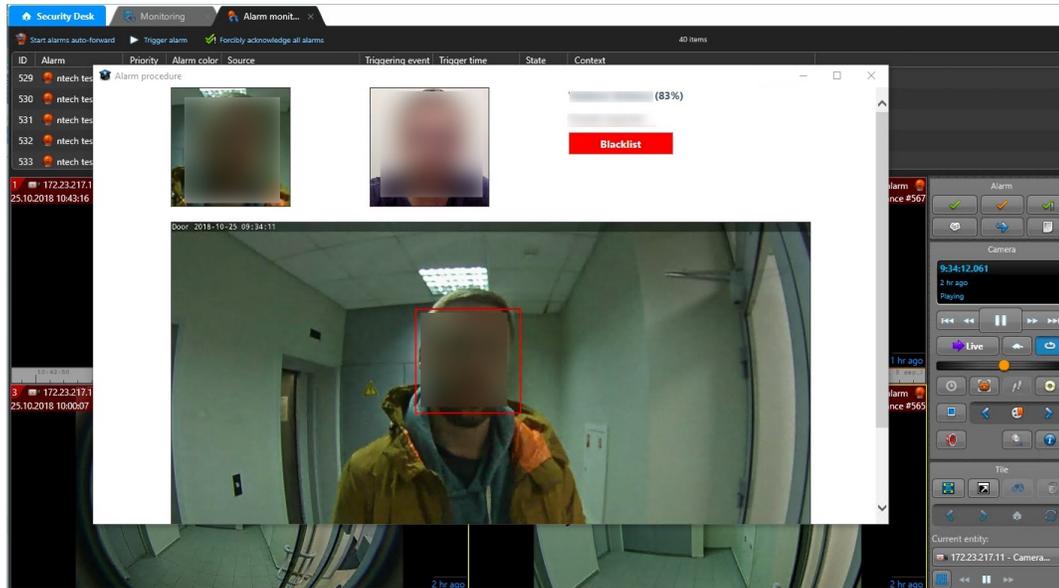
После настройки точек доступа и импорта камер завершите интеграцию, создав *базу данных досье*. После этого оповещения о событиях распознавания лиц будут автоматически отправляться в Genetec Security Center. См. *Оповещения в Genetec Security Center*.

Оповещения в Genetec Security Center

Каждое событие распознавания лица с камеры Genetec, для которого найдено досье, активирует соответствующее оповещение **alarm** в Genetec Security Center. Каждое оповещение, отправленное FindFace Security, связывается с камерой-источником события распознавания лица, поэтому вы можете сразу же просматривать живое или архивное видео в задаче Alarm Monitoring в Genetec Security Desk. FindFace

Security также использует операции с оповещением Alarm Procedures для обеспечения пользователя дополнительными данными по событию, такими как:

- обнаруженное на видео лицо
- найденное похожее лицо из базы данных досье
- имя человека и комментарий из досье
- степень схожести лиц (уверенность алгоритма в совпадении)
- имя списка наблюдения
- полный кадр



Обработка полученного оповещения о распознавания лица выполняется аналогично другим оповещениям в Genetec Security Center.

1.3.2 Аххон Next

Интеграция FindFace Security с программным комплексом Аххон Next позволяет обрабатывать видеопотоки из системы безопасности на базе Аххон и анализировать их на предмет наличия лиц из досье.

Важно: Один экземпляр FindFace Security поддерживает работу не более чем с одним сервером Аххон Next.

Интеграция с Аххон Next выполняется с использованием плагина `ffsecurity_axhon`.

Для того чтобы настроить интеграцию с Аххон Next в ОС Ubuntu, выполните следующие действия:

1. Активируйте плагин, добавив в файл конфигурации `/etc/ffsecurity/config.py` строку `INSTALLED_APPS.append('ffsecurity_axhon')`.

```
sudo vi /etc/ffsecurity/config.py
```

```
...
```

(continues on next page)

(продолжение с предыдущей страницы)

```
# integration plugins
INSTALLED_APPS.append('ffsecurity_axxon') # remove or comment out this line to disable
```

- В файл конфигурации добавьте секцию FFSECURITY->AXXON. Заполните ее так, как показано в примере ниже. В параметре `api` укажите адрес сервера Аххон Next, по которому FindFace Security будет обращаться к API Аххон и за HLS-потоками архива. В параметре `rtsp` укажите общий адрес видеопотоков на сервере Аххон Next.

```
FFSECURITY = {
'AXXON': {
  'api': 'http://user:password@example.com/',
  'rtsp': 'rtsp://user:password@example.com:554/',
  }
}
```

- (Опционально). Если в событиях распознавания лиц требуется отображать клипы видео из Аххон Next, отредактируйте секцию FFSECURITY_UI_CONFIG так, как показано в примере ниже.

```
FFSECURITY_UI_CONFIG = {
  'dossier': {
    'video': True,
  }
}
```

- Создайте камеры в FindFace Security (см. *Управление видеокамерами*). При создании камер вам потребуется ввести их URL в формате `axxon:<friendlyNameLong>`, где `friendlyNameLong` - имя камеры на сервере Аххон Next. Данное имя можно посмотреть в интерфейсе Аххон, или через API Аххон, выполнив команду:

```
curl http://user:password@127.0.0.1/video-origins/

{
  "OLOLOE-DEV/DeviceIpint.vhod_1/SourceEndpoint.video:0:0" : {
    "friendlyNameLong" : "vhod_1.Vhod_1",
    "friendlyNameShort" : "Vhod_1",
    "origin" : "OLOLOE-DEV/DeviceIpint.vhod_1/SourceEndpoint.video:0:0",
    "state" : "signal_restored"
  }
}
```

Для единственной камеры из примера выше URL должен быть задан как `axxon:vhod_1.Vhod_1`.

На этом настройка интеграции будет завершена. Если интеграция настроена корректно, FindFace Security будет выполнять проверку наличия лиц из досье в видеопотоках Аххон Next, а в событиях распознавания лиц будут отображаться клипы видео из Аххон Next (при соответствующих настройках).