
FindFaceSecurity

Выпуск 1.0

NtechLab

июн. 26, 2023

Содержание

1	Полное руководство	1
1.1	Руководство администратора	1
1.2	Руководство оператора	27

Система распознавания лиц FindFace Security предназначена для автоматизации основной деятельности сотрудников служб безопасности и гостеприимства при построении взаимоотношений с посетителями.

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

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

- снижение операционных потерь от мошеннических действий клиентов и посетителей;
- снижение репутационных потерь и предотвращение конфликтных ситуаций;
- повышение качества обслуживания клиентов, в частности VIP-гостей.

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

Примечание: Документ доступен по адресу <https://docs.findface.pro/ffsec/ru/latest/index.html> и во встроеном фреймворке http://<ffsecurity_ip>/doc/ (после установки).

1.1 Руководство администратора

1.1.1 Системные требования

FindFace Security разворачивается на одиночном сервере или нескольких серверах. Для расчета характеристик сервера(ов) используйте следующие требования:

Требование	Описание
Процессор	Intel Xeon E5 с поддержкой AVX или аналогичный ему процессор. Характеристики зависят от количества камер. Для одной камеры 1080p@25FPS требуется 2 ядра с HT с частотой >2 ГГц под обработку видео и 2 ядра с HT с частотой >2ГГц под распознавание лиц.
Память	Потребление памяти зависит от количества камер. Для одной камеры 1080p@25FPS требуется 4 ГБ под обработку видео и 4 ГБ под распознавание лиц.
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	Ubuntu 16.04 LTS (64-битная)

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.

1.1.2 Архитектура

FindFace Security разворачивается на одиночном сервере или нескольких серверах.

Совет: См. *Системные требования*.

Для установки FindFace Security используются следующие установочные пакеты:

- Пакет с компонентами `<findface-security-repo>.deb`.
- Пакеты с моделями нейронных сетей для извлечения биометрических образцов лиц `<findface-data>.deb`.

Работоспособность FindFace Security обеспечивается взаимодействием следующих компонентов:

Компонент	Описание
PostgreSQL	База данных (СУБД), в которой хранятся детализированные досье посетителей с разбиением по категориям (спискам наблюдения), биометрические данные посетителей, а также все события распознавания лиц. Помимо этого, в базе данных хранится информация внутреннего характера: профили пользователей FindFace Security, данные видеокамер и пр. Устанавливается из репозитория Ubuntu (наряду с Redis).
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 видеодетектора <code>fkvideo_detector</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. Систему можно таким образом, что событие будет записываться и отображаться в веб-интерфейсе только в том случае, если степень схожести обнаруженного лица и лица из какого-либо досье превышает предустановленное пороговое значение, т. е. если лица совпадают (параметр <code>IGNORE_UNMATCHED</code> в файле <code>/etc/ffsecurity/config.py</code> , см. <i>Установка базовой конфигурации</i>). Сервис <code>ffsecurity</code> также отвечает за поиск лиц в базе событий.
fkvideo_detector	Видеодетектор лиц, который обнаруживает лицо «на лету» в видеопотоке 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. Для работы необходимы пакеты с моделями нейронных сетей <code><findface-data>.deb</code> .
findface-postgres-facen	Расширение к базе данных PostgreSQL, которое используется для вычисления степени схожести обнаруженного лица с лицами из досье путем сравнения биометрических образцов.
Веб-интерфейс	Веб-интерфейс <code>ffsecurity-ui</code> используется для отображения результатов работы системы распознавания лиц, управления видеокамерами, пользователями, ведения списков наблюдения, поиска лиц в базе событий и социальных сетях.
NTLS	Локальный сервер лицензий с управлением через веб-интерфейс, взаимодействующий для верификации лицензий с глобальным сервером лицензий NtechLab или аппаратным лицензионным ключом.

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

Примечание: Для очистки базы данных от устаревших событий используйте *утилиту* `event-cleaner`.

1.1.3 Развертывание FindFace Security

Для вашего удобства мы предлагаем 2 варианта развертывания FindFace Security. Выберите наиболее подходящий вариант в зависимости от выбранной вами архитектуры:

- Развертывание на группе серверов может быть только пошаговым.
- Развертывание на одиночном сервере может быть выполнено как пошагово, так и из консольного инсталлятора.

Пошаговое развертывание

Данный раздел содержит сведения о пошаговом развертывании компонентов FindFace Security на одиночном сервере. 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:

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

Установка необходимого стороннего ПО

Для работы 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
```

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 локального 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 локальный 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
```

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 веб-интерфейса) 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. Придумайте токен для авторизации видеодетектора лиц в сервисе `ffsecurity` и укажите его в параметре `VIDEO_DETECTOR_TOKEN` (данный токен также нужно будет продублировать в *настройках видеодетектора*).

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': -7, что означает, что в досье могут быть загружены лица в любом качестве.

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

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

EXTERNAL_ADDRESS="192.168.104.204"

DEBUG = False

LANGUAGE_CODE = 'ru-ru'

TIME_ZONE = 'UTC'

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

FFSECURITY = {
    'VIDEO_DETECTOR_TOKEN': 'Ghj545dfd',
    'CONFIDENCE_THRESHOLD': 0.75,
    'MINIMUM_DOSSIER_QUALITY': -0.1,
    'IGNORE_UNMATCHED': False,
    'EXTRACTION_API': 'http://127.0.0.1:18666/'
}
```

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

- 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
```

- 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
```

9. 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 `fkvideo_detector` и `extraction-api`) выполняется следующим образом:

1. Установите видеодетектор лиц.

```
sudo apt install -y fkvideo-detector
```

2. Откройте файл конфигурации видеодетектора и отредактируйте в нем следующие настройки:

Примечание: Обратите внимание, что в параметре `api-token` нужно указать значение `VIDEO_DETECTOR_TOKEN` из `/etc/ffsecurity/config.py` (см. *Установка базовой конфигурации*).

```
sudo vi /etc/fkvideo.ini

api-url=127.0.0.1:8002

api-token=<'VIDEO_DETECTOR_TOKEN'>

detector-name=detector1

request-url=/video-detector/frame/

camera-url=/video-detector/cameras/

realtime=0
```

Важно: По умолчанию видеодетектор подбирает лучшее изображение лица в режиме реального времени (`realtime=1`). В этом режиме видеодетектор начинает отправлять в `ffsecurity` изображения лица сразу после его появления в поле зрения видеокамеры. Для более эффективного

подбора лучшего изображения лица рекомендуется установить буферный режим (`realtime=0`). В буферном режиме видеодетектор использует меньший объем дискового пространства, поскольку для каждого лица отправляет в `ffsecurity` только одно изображение, но наивысшего качества.

3. Добавьте сервис `fkvideo_detector` в автозагрузку Ubuntu и запустите его. Убедитесь, что сервис активен.

```
sudo systemctl enable fkvideo_detector@fkvideo && sudo systemctl start fkvideo_
↔detector@fkvideo

sudo systemctl status fkvideo_detector@fkvideo
```

4. Установите компонент `extraction-api`.

```
sudo apt install -y findface-extraction-api
```

5. 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
```

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

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

```
models:
  gender: ""
  age: ""
  emotions: ""
```

7. Добавьте сервис `extraction-api` в автозагрузку Ubuntu и запустите его. Убедитесь, что сервис активен.

```
sudo systemctl enable findface-extraction-api && sudo systemctl start findface-extraction-api

sudo systemctl status findface-extraction-api
```

Развертывание из консольного инсталлятора

Для развертывания FindFace Security на одиночном сервере 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 любую папку на сервере установки (например, `/home/username`).
3. Из данной папки 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-facem	Устанавливается и запускается.
ffsecurity	Устанавливается и запускается.
ffsecurity-ui	Устанавливается и запускается.
fkvideo_detector	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.
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.

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.

защиту.

Примечание: Базовый адрес задается в параметре EXTERNAL ADDRESS в файле конфигурации /etc/ffsecurity/config.py.

Важно: Для первого входа в систему после развертывания FindFace Security используйте учетную запись администратора admin, которая была создана при установке *базовой конфигурации*.

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

- Управление группами камер. Добавление и настройка камеры. См. *Управление видеокameraми*.
- Управление списками досье. Создание досье вручную и пакетно. См. *Управление базой данных посетителей*.
- Управление пользователями FindFace Security. См. *Управление пользователями*.
- Работа с событиями распознавания лиц и поиск лиц в базе событий и социальных сетях (см. Руководство оператора).

1.1.5 Управление видеокameraми

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

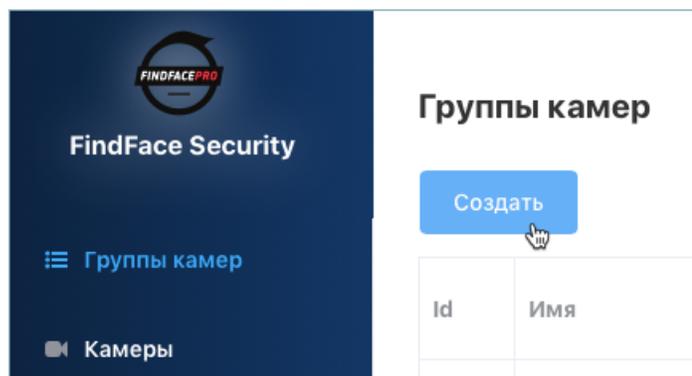
В этой главе:

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

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.

Создать группу камер

* Имя

Комментарий

Дедуплицировать события

* Интервал дедубликации

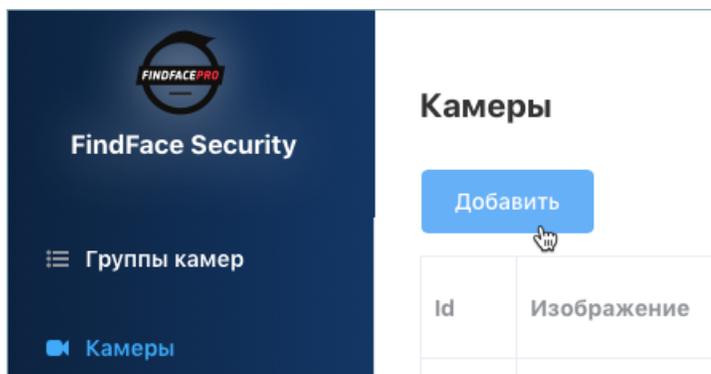
Активная

4. Если события от камер, принадлежащих одной группе, требуется дедуплицировать, т. е. исключить одинаковые события, поставьте флажок *Дедуплицировать события* и задайте интервал дедубликации (интервал, с которым события проверяются на уникальность).
5. Поставьте флажок *Активная*.
6. Нажмите на кнопку *Сохранить*.

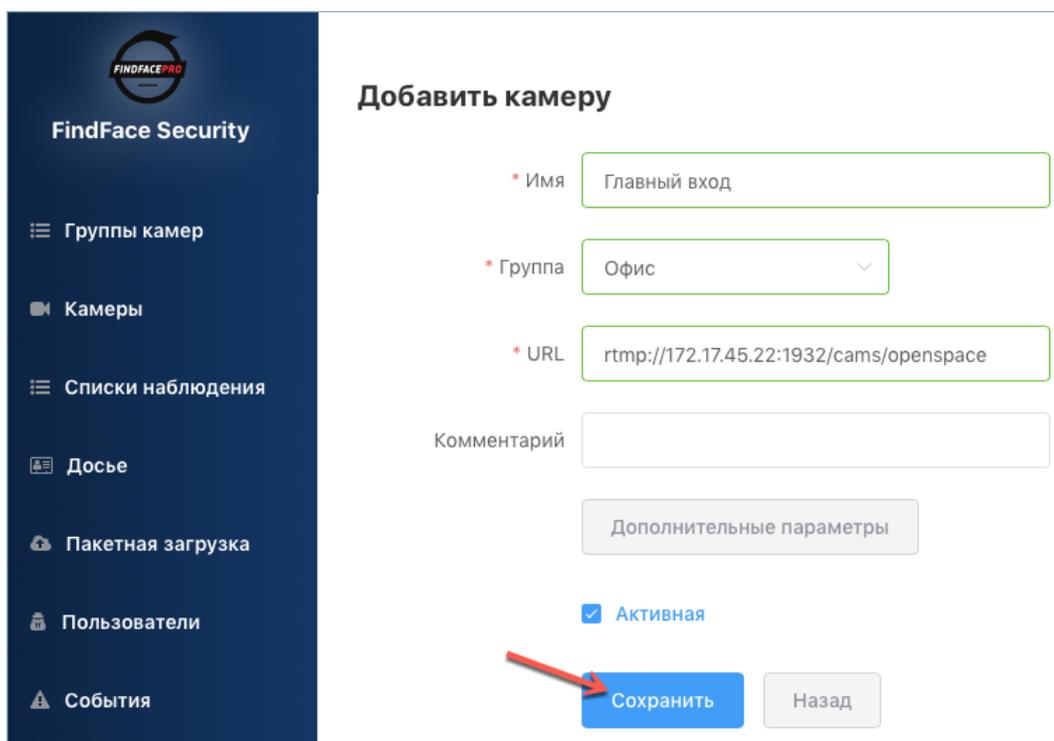
Добавление камеры в группу

Для добавления камеры в группу выполните следующие действия:

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



2. Нажмите на кнопку *Добавить*.
3. Введите название камеры и добавьте ее в одну из групп. При необходимости введите комментарий к камере.



4. Задайте URL камеры.
5. При необходимости включите детектирование и отслеживание лиц только внутри заданной прямоугольной области, задав параметр `ROT`. Используйте данную опцию, чтобы уменьшить нагрузку на `fkvideo_detector`.

Регион захвата лица (ROI):							
X	<input type="text" value="50"/>	Y	<input type="text" value="50"/>	Ширина	<input type="text" value="100"/>	Высота	<input type="text" value="100"/>
Регион слежения (ROT):							
X	<input type="text" value="30"/>	Y	<input type="text" value="30"/>	Ширина	<input type="text" value="150"/>	Высота	<input type="text" value="150"/>

- При необходимости включите отправку в компонент `ffsecurity` только тех лиц, которые были обнаружены внутри интересующей области ROI.
- Поставьте флажок *Активная*.
- Нажмите на кнопку *Сохранить*.

1.1.6 Управление базой данных посетителей

На каждого нежелательного посетителя и VIP-гостя в FindFace Security создается досье, содержащее одну или несколько фотографий. Досье 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 посетителя.

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

В этой главе:

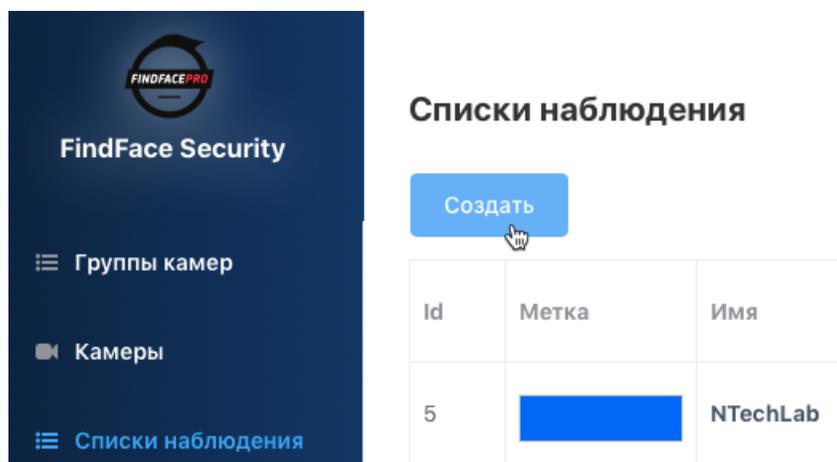
- *Списки наблюдения*
 - *Создание списка*
 - *Деактивация или удаление списка*
 - *Просмотр досье из списка*
- *Создание досье вручную*
- *Пакетная загрузка фотографий*

Списки наблюдения

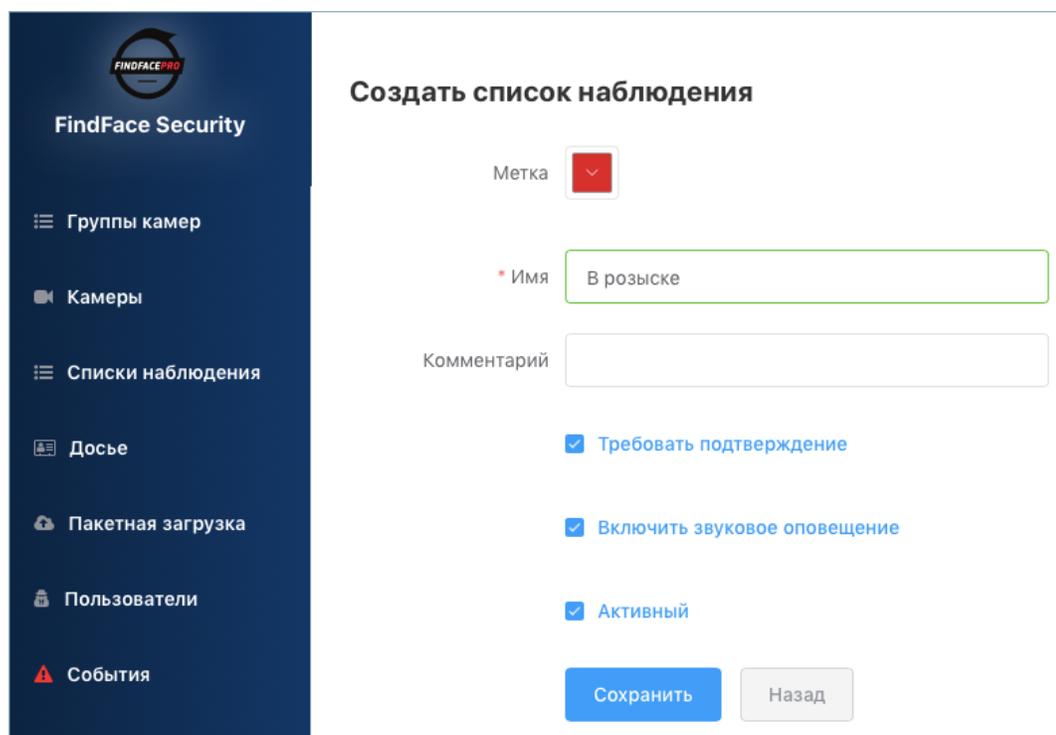
Создание списка

Для создания списка наблюдения выполните следующие действия:

- 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 посетителей 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*.

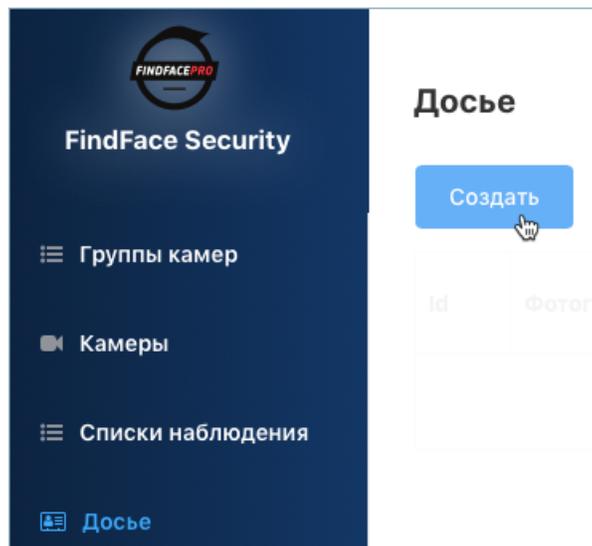
Просмотр досье из списка

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 вручную выполните следующие действия:

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



2. Нажмите на кнопку *Создать*.
3. Добавьте фотографию и введите имя посетителя. При необходимости добавьте комментарий.

Важно: Фотография должна отвечать следующим требованиям:

- Содержать лицо и притом только одно.
- Лицо должно быть надлежащего качества, т. е. в близком к анфас положении.

При несоответствии фотографии одному или нескольким требованиям будет выведено сообщение с описанием ошибки.

The screenshot shows the 'Создать досье' (Create Profile) interface. On the left is a dark blue sidebar with the 'FindFace Security' logo and menu items: Группы камер, Камеры, Списки наблюдения, Досье, Пакетная загрузка, Пользователи, События, and Поиск. The main content area is titled 'Создать досье' and contains the following elements:

- Фотографии:** A section with the label 'Фотографии' containing a preview of a woman's face and a large white square with a black plus sign for adding more photos.
- Имя:** A text input field with a red asterisk, containing the text 'Кейт Остин'.
- Комментарий:** A text input field.
- Списки наблюдения:** A dropdown menu with a red asterisk, currently showing 'В розыске' with a close button and a dropdown arrow.
- Активное:** A checked checkbox labeled 'Активное'.
- Buttons:** A blue 'Сохранить' (Save) button and a grey 'Назад' (Back) button.

4. Из раскрывающегося списка *Списки наблюдения* выберите список (или несколько списков, по очереди), в который следует добавить досье.
5. 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

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

Старт

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. Для запуска пакетного создания досье нажмите на кнопку *Старт*.

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 посетителей, событий, пользователями FindFace Security.*

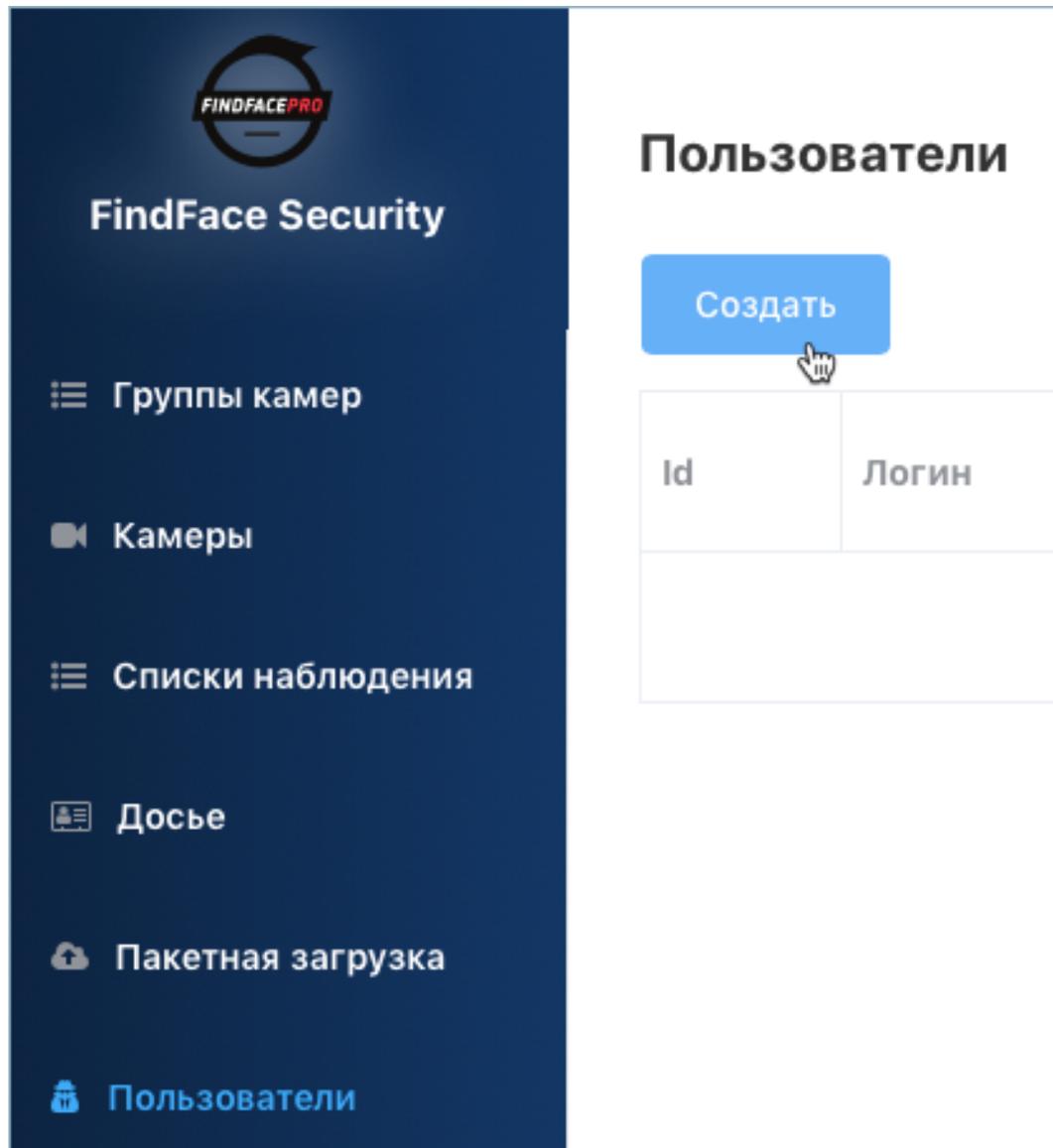
Важно: Первый *созданный из консоли* администратор (Супер Администратор) не может лишиться прав даже при смене роли.

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

Создание пользователя

Для создания нового пользователя выполните следующие действия:

1. Нажмите на кнопку *Создать*.



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:

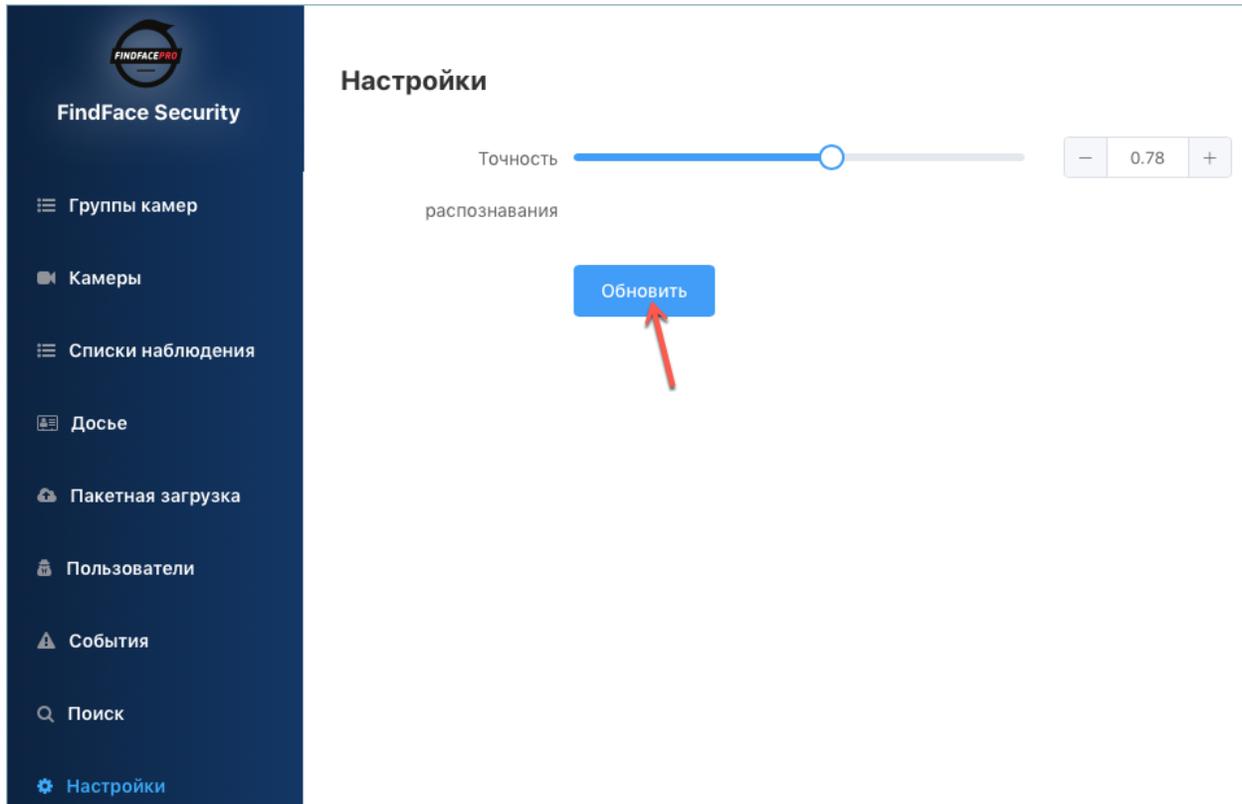
1. Щелкните по логину пользователя в списке.
2. Для деактивации снимите флажок *Активный*. Нажмите на кнопку *Обновить*.
3. Для удаления нажмите на кнопку *Удалить*.

1.1.8 Настройка точности распознавания лиц

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.



Совет: Систему можно настроить таким образом, что событие будет записываться и отображаться в веб-интерфейсе только в том случае, если лица совпадают (параметр `IGNORE_UNMATCHED` в файле `/etc/ffsecurity/config.py`, см. *Установка базовой конфигурации*).

1.1.9 Очистка базы данных событий с `event-cleaner`

Для удаления устаревших событий используйте утилиту `event-cleaner`.

Справка по утилите вызывается следующей командой:

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

```
usage: findface-security-manage 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
```

(continues on next page)

(продолжение с предыдущей страницы)

```

--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
```

1.1.10 Обслуживание и устранение неисправностей

Аудит-логи

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

Важно: Для того чтобы включить хранение аудит-логов на жестком диске, 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, выполните следующую команду:

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

При расшифровке аудит-логов в первую очередь обращайте 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=e26016;
↪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-manage 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.

```

Пт 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-manage runworker
  _SYSTEMD_SLICE=system-findface\x2dsecurity\x2dworker.slice
  _PID=6588

```

(continues on next page)

(продолжение с предыдущей страницы)

```

_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 вместе с базой данных с помощью скрипта `ffsecurity_uninstall.sh`. Перед удалением будут созданы резервные копии файлов конфигурации и базы данных FindFace Security.

Выполните следующие действия:

1. Загрузите скрипт `ffsecurity_uninstall.sh` в любую папку на сервере установки (например, в `/home/username/`).
2. Из данной папки сделайте скрипт `ffsecurity_uninstall.sh` исполняемым.

```
chmod +x ffsecurity_uninstall.sh
```

3. Запустите скрипт `ffsecurity_uninstall.sh`.

```
sudo ./ffsecurity_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

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

# redirect from http to https version of the site
server {
    listen 80;
    server_name my-example-domain.com www.my-example-domain.com;
    rewrite ^(.*) https://my-example-domain.com$1 permanent;
    access_log off;
}

server {
    listen 443 ssl;
    server_name my-example-domain.com;

    ssl_certificate /etc/nginx/ssl/my-example-domain.com.crt;
    ssl_certificate_key /etc/nginx/ssl/my-example-domain.com.key;

    root /usr/share/ffsecurity-ui

    location / {
        try_files $uri $uri/ @ffsec;
    }

    location @ffsec {
        proxy_pass http://127.0.0.1:8002;
    }
}
```

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"
```

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:

- Работа с досье на посетителя. См. *Работа с досье на посетителя* (только для пользователей с правами оператора).
- Работа с событиями распознавания лиц. См. *Работа с событиями распознавания лиц*.
- Поиск лиц в базе событий и социальных сетях. См. *Поиск лица в списке событий и соцсетях*.

1.2.2 Работа с досье на посетителя

На каждого нежелательного посетителя и VIP-гостя в FindFace Security создается досье, содержащее одну или несколько фотографий. Досье классифицируется по принадлежности к тому или иному списку наблюдения.

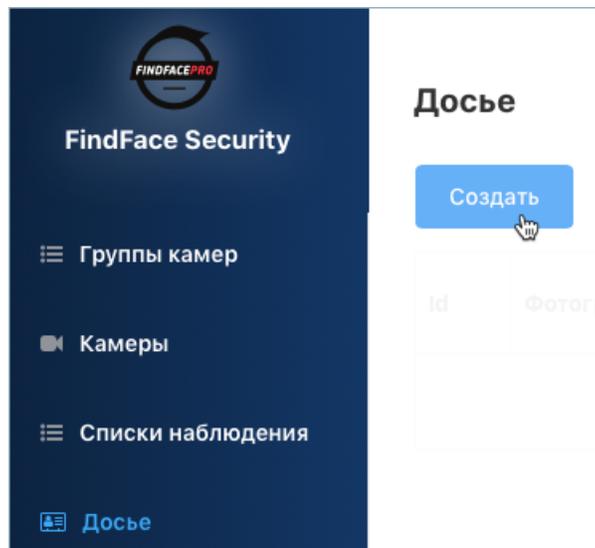
В этой главе:

- *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 фотографию и введите имя посетителя. При необходимости добавьте комментарий.

Важно: Фотография должна отвечать следующим требованиям:

- Содержать лицо и притом только одно.
- Лицо должно быть надлежащего качества, т. е. в близком к анфас положении.

При несоответствии фотографии одному или нескольким требованиям будет выведено сообщение с описанием ошибки.

The screenshot shows the 'Создать досье' (Create Profile) 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, Пользователи, События, and Поиск. The main content area is titled 'Создать досье' and contains the following elements:

- Фотографии:** A section with the label 'Фотографии' containing a photo of a woman and a placeholder with a plus sign.
- Имя:** A text input field with a red asterisk and the value 'Кейт Остин'.
- Комментарий:** A text input field.
- Списки наблюдения:** A dropdown menu with a red asterisk, currently showing 'В розыске' and a close button.
- Активное:** A checked checkbox labeled 'Активное'.
- Buttons:** A blue 'Сохранить' (Save) button and a grey 'Назад' (Back) button.

4. Из раскрывающегося списка *Списки наблюдения* выберите список (или несколько списков, по очереди), в который следует добавить досье.
5. 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.

1.2.3 Работа с событиями распознавания лиц

Работа с событиями распознавания лиц, в том числе просмотр истории, выполняется на вкладке *События*.

Совет: Поиск лица в списке событий, а также в социальных сетях выполняется на вкладке *Поиск*.

В этой главе:

- Работа со списком событий
- Карточка события. Принятие события
- Карточка события. Поиск лица

Работа со списком событий

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 22323 [События](#) [Социальные сети](#)

Имя (50)

Точность 76%

распознавания

Комментарий

Время 2018-04-09 16:40:40

Камера **Entrance 5F**

Группа камер **NTL Office**

Списки наблюдения **NTechLab**

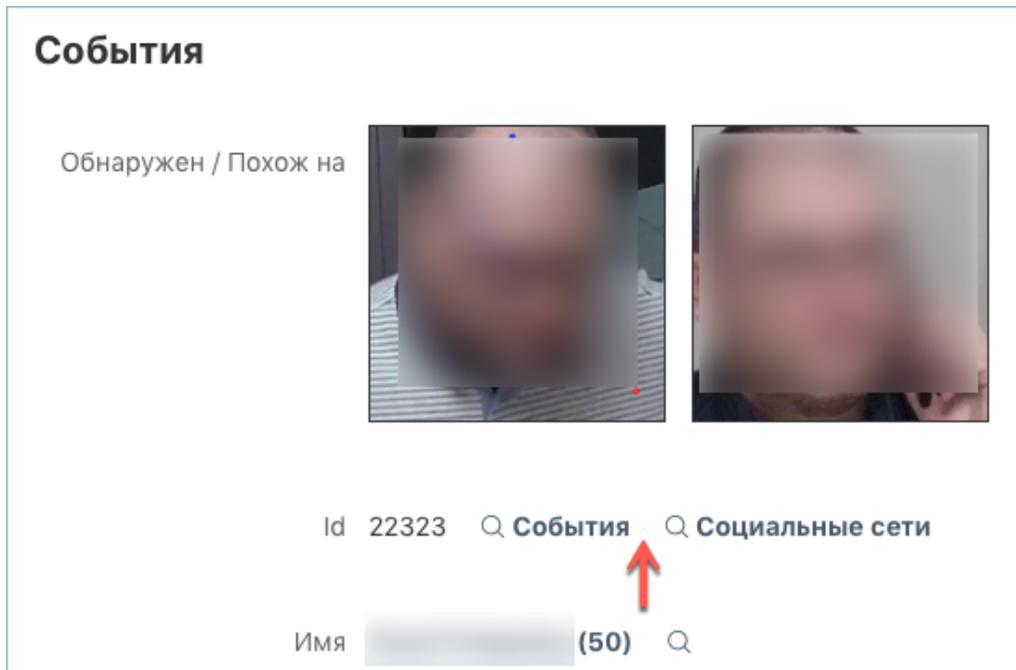
Подтверждение событие

Сохранить

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

Карточка события. Поиск лица

FindFace Security позволяет искать обнаруженные на видео лица во внутренней (список событий) или внешней (соцсеть ВКОНТАКТЕ) базах данных. Для перехода на вкладку поиска из карточки события нажмите *События* или *Социальные сети*.



См.также:

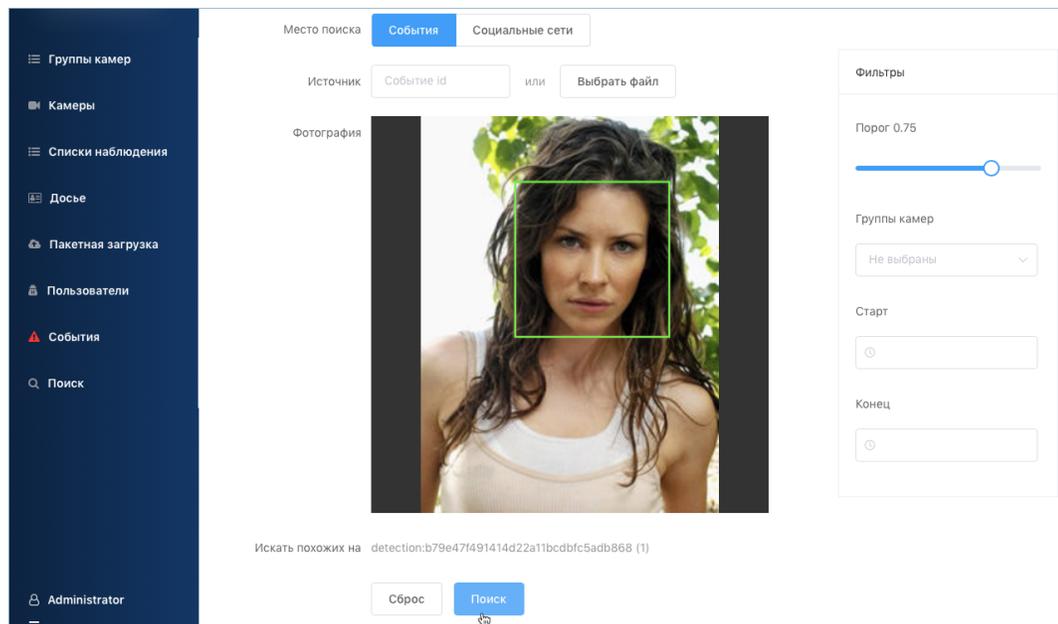
- Поиск лица в списке событий и соцсетях.

1.2.4 Поиск лица в списке событий и соцсетях

FindFace Security позволяет искать лица во внутренней (список событий) и внешней (соцсеть ВКонтакте) базах данных. Искать можно как по ID события, так и по фотографии.

Для поиска лица выполните следующие действия:

1. Перейдите на вкладку *Поиск*.



2. Укажите место поиска: *События* или *Социальные сети*.
3. Укажите ID события, лицо из которого нужно найти, или загрузите фотографию. Видеокадр события/фотография будут отображены в поле *Фотография*. Если на изображении присутствует несколько лиц, выберите нужное.
4. По умолчанию в результатах поиска отображаются лица, степень схожести которых с искомым равна или превышает 0.75. При необходимости измените данное значение.
5. Если поиск выполняется в списке событий, при необходимости укажите группу камер и период времени, в течение которого произошло событие.
6. Нажмите *Поиск*. Результаты поиска будут отображены ниже. Для каждого найденного лица будет указана вероятность его совпадения с лицом из события/на исходной фотографии.