



**Бастион-3 – SecurOS FaceX. Руководство
администратора**

Версия 2024.1

(19.08.2024)



Самара, 2023



Оглавление

1. Общие сведения.....	3
1.1. Назначение и область применения.....	3
1.2. Условия применения.....	3
1.2.1. Требования к совместимости.....	3
1.2.2. Лицензирование системы.....	4
2. Установка системы.....	4
3. Настройка системы.....	4
3.1. Настройка СБИ SecurOS FaceX.....	4
3.2. Настройка драйвера.....	9
3.2.1. Основные настройки.....	10
3.2.2. Настройка соединений с серверами SecurOS FaceX.....	10
3.2.3. Настройка работы с камерами.....	12
3.2.4. Точки прохода.....	15
4. Работа в штатном режиме.....	19
4.1. Операции с пропусками.....	19
4.2. Режим идентификации.....	20
5. Нештатные ситуации.....	23
6. Приложения.....	24

1. Общие сведения

1.1. Назначение и область применения

Модуль «Бастион-3 – SecurOS FaceX» предназначен интеграции ПК «Бастион-3» с системой биометрической идентификации (СБИ) SecurOS FaceX.

Основной функцией модуля является обеспечение доступа посетителей через точки прохода системы контроля и управления доступом (СКУД) ELSYS (ООО «ЕС-пром», ГК «ТвинПро») путём сопоставления изображения лица человека, полученного с камеры видеонаблюдения с его фотографией, сохранённой в ПК «Бастион-3».

Модуль позволяет использовать как режим двухфакторной аутентификации (по изображению лица с прикладыванием карты доступа к считывателю), так и режим идентификации по изображению лица. Одновременно могут быть заданы различные режимы доступа для разных точек прохода.

Доступ на выбранных точках прохода возможен для посетителей с пропусками любых категорий.

Дополнительно, модуль предоставляет возможность создавать *виртуальные точки прохода*.

Виртуальная точка прохода не связана с реальным преграждающим устройством, но позволяет отслеживать местоположение персонала и посетителей в зонах, контролируемых камерами видеонаблюдения, подключенных к серверу SecurOS FaceX.

1.2. Условия применения

1.2.1. Требования к совместимости

На модуль «Бастион-3 – SecurOS FaceX» распространяются те же требования к аппаратной и программной платформе, что и для ПК «Бастион-3».

Для работы с реальными точками прохода требуется наличие СКУД ELSYS и драйвера «Бастион-3 – Elsys».

Для работы доступа в режиме идентификации версия прошивки KCK MB-NET должна быть не меньше 2.12, версия прошивки контроллера ELSYS-MB должна быть не меньше 2.68.

Контроллеры ELSYS-MB-SM не могут быть использованы ни для режима идентификации, ни для режима двухфакторной аутентификации.

Необходимо, чтобы была установлена версия ПО SecurOS — 10.9 и выше. Обмен данными между модулем «Бастион-3 – SecurOS FaceX» и СБИ SecurOS FaceX выполняется по протоколу HTTP.

Модуль совместим с ПК «Бастион-3» версии 2023.1 и выше. Для работы модуля необходимо иметь установленную версию .Net версии 6.0.

1.2.2. Лицензирование системы

Для работы модуля требуется отдельная лицензия. Лицензирование производится по числу обслуживаемых системой *направлений прохода*. Исп. 1 предназначено для работы на 1 точке прохода в 1 направлении (вход или выход), либо для организации одной виртуальной точки прохода. Например, для организации двухфакторной аутентификации для одного турникета в обоих направлениях потребуется 2 лицензии на модуль «Бастион-3 – SecurOS FaceX Исп. 1». Число необходимых лицензий не зависит от числа используемых видеокамер.

2. Установка системы

Для работы системы необходимо установить драйвер «Бастион-3 – SecurOS FaceX». Модуль может устанавливаться как в составе ПК «Бастион-3», так и отдельно от него.

Установка в ОС Windows производится путем запуска файла инсталлятора SecurOsFaceXSetup.msi.

В ОС на базе Linux драйвер поставляется в виде установочного пакета формата DEB или RPM с именем `bastion3-driver-securosfacex_*`. Драйвер устанавливается в каталог `/opt/bastion3/Drivers/SecurOsFaceX`.

3. Настройка системы

3.1. Настройка СБИ SecurOS FaceX

На сервере SecurOS должны быть настроены подключения ко всем камерам, которые планируется использовать в СКУД. Подключенные к СБИ SecurOS FaceX камеры затем необходимо будет привязать к точкам прохода СКУД и виртуальным точкам прохода в конфигурации драйвера «Бастион-3 – SecurOS FaceX».

В настройках объекта "Компьютер <имя видеосервера SecurOS>" должен быть задан IP-адрес видеосервера (Рис. 1):

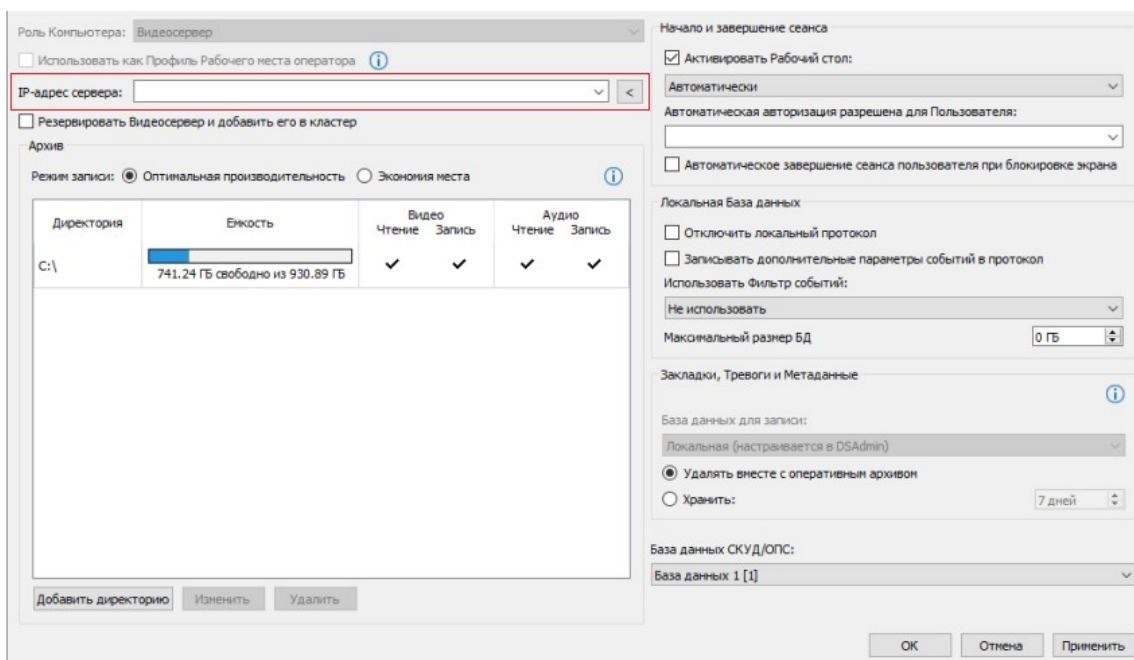


Рис. 1: Настройка сервера SecurOS

На сервере SecurOS должен быть создан пользователь (Рис. 2):

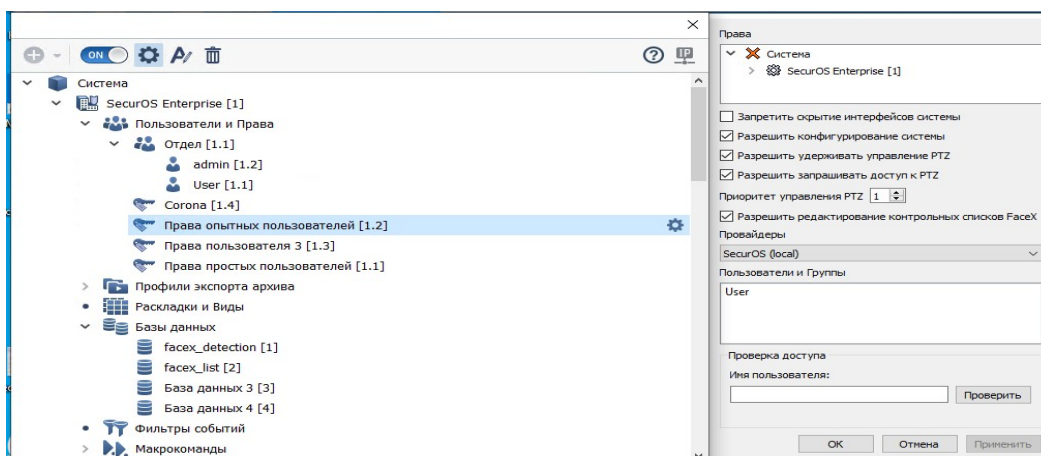


Рис. 2: Пользователь с правами на сервере SecurOS

Для работы модуля необходимо, чтобы на сервере «FaceX» были созданы и настроены БД детекций (например `face_x_detect`) и БД контрольных списков (например `face_x_list`). Необходимо указать ip-адрес сервера, порт и пароль. Значения по умолчанию: пароль — `postgres`, порт - 5432 (Рис. 3).

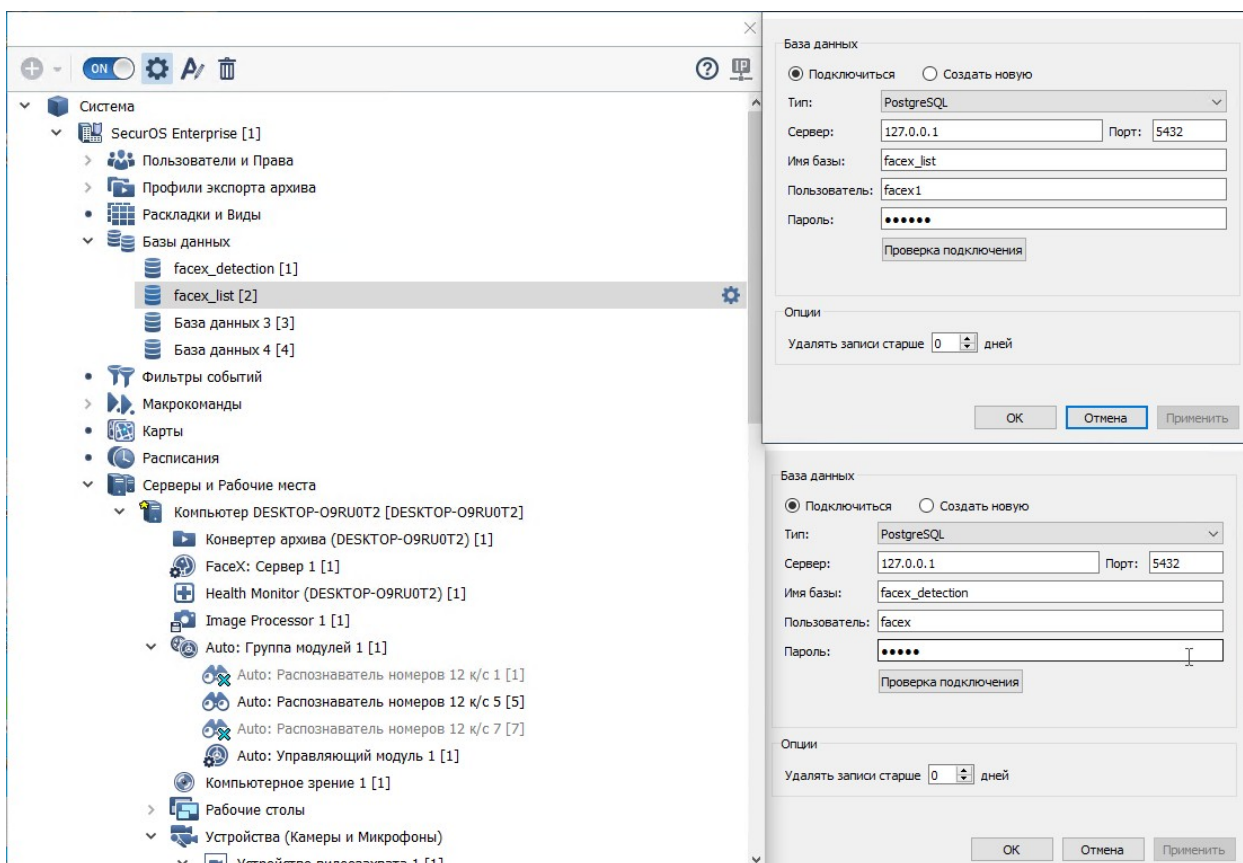


Рис. 3: Создание БД «детекций» и БД «контрольных списков»

В СБИ SecurOS FaceX должен быть создан объект «Face X: Сервер» (Рис. 4).

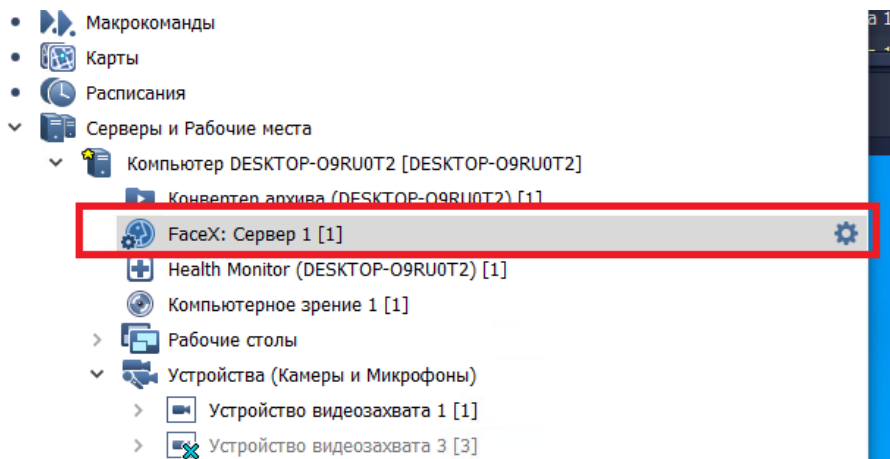


Рис. 4: Создание объекта «FaceX: Сервер»

Для настройки созданного объекта необходимо открыть меню настроек (Рис. 5).

Общие настройки | Камеры

БД детекций и распознаваний:

БД контрольных списков:

Резервная БД контрольных списков:

Режим распознавания:

Порт:

Порог уверенности детекции лица:

Период детектирования:

Максимальное время потери трека:

Максимальное время ожидания лучшего лица:

Период обновления лучшего лица:

Режим взаимодействия со СКУД

Однофакторная СКУД-аутентификация

Многофакторная СКУД-аутентификация

Время ожидания верификации:

Порог подобия для режима СКУД:

Дополнительные

Размер очереди заданий:

Количество вычислительных потоков:

Количество потоков сетевого транспорта:

Размер очереди кадров (на камеру):

Период синхронизации с БД контрольных списков:

Дополнительный фильтр детекций

Событие о положении лица на каждом кадре

Событие о нераспознанном лице

Рис. 5: Общие настройки объекта «FaceX: Сервер»

Поле «Порт» будет использоваться в параметрах подключения к серверу «FaceX». По умолчанию имеет значение 21093.

В разделе «Режим взаимодействия со СКУД» настраивается тип аутентификации.

Если предполагается работа драйвера «Бастион-3 – SecurOS FaceX» только в режиме идентификации (проход по лицу или карте), то необходимо выбрать только режим «Однофакторная СКУД-аутентификация».

Для работы двухфакторной аутентификации (проход в режиме «лицо после карты» или «карта после лица») необходимо включить оба режима аутентификации. После включения режима «Многофакторная СКУД-аутентификация» станут доступными дополнительные настройки. Время ожидания верификации нужно установить не менее 50000 мс, порог подобия для режима СКУД не менее 60.

Так как драйвер «Бастион-3 – SecurOS FaceX» поддерживает работу с несколькими камерами, подключенными к одному серверу распознавания SecurOS FaceX, рекомендовано сразу включить и настраивать оба режима аутентификации на сервере SecurOS FaceX.

Далее необходимо перейти на страницу «Камеры» (Рис. 6).

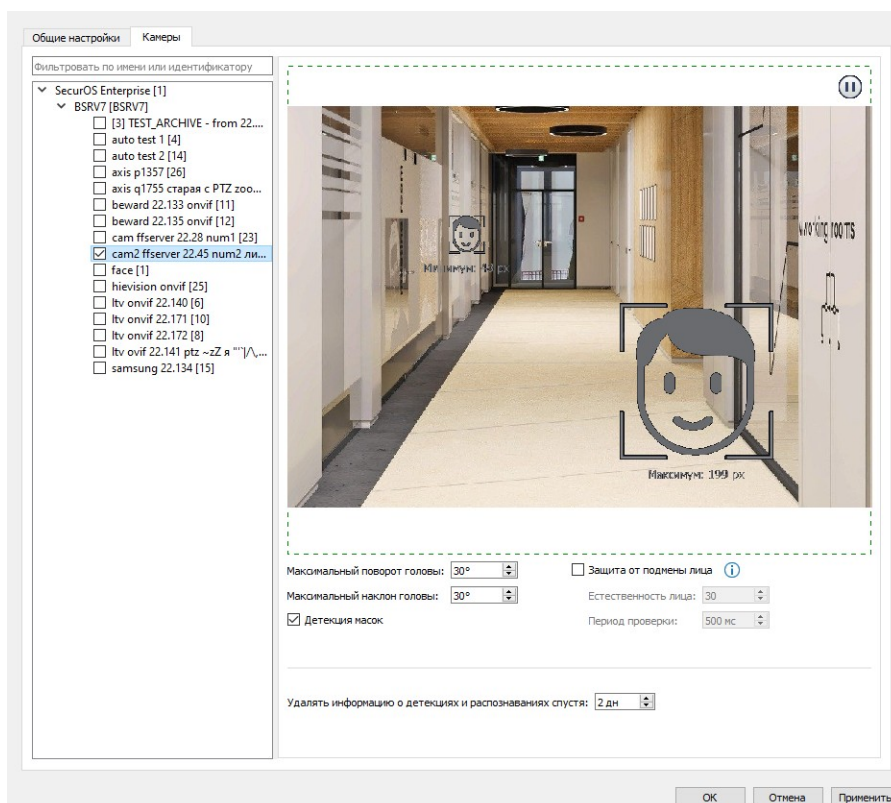


Рис. 6: Выбор списка камер для объекта «FaceX: Сервер»

На вкладке камеры необходимо выбрать список камер для распознавания лиц и произвести их настройку. (см. «SecurOS FaceX. Руководство пользователя.pdf», 3.2 Настройка FaceX: Сервер).

При активации опции «Защита от подмены лиц» СКУД не будет предоставлять доступ тем персонам, у которых параметр «Естественность лица», полученный входе распознавания, меньше установленного значения на сервере.

При включении опции «Детектор масок» при распознавании лиц будет выполняться проверка на наличие или отсутствие на лице медицинской маски.

Далее на сервере SecurOS необходимо создать объект REST API (Рис. 7).

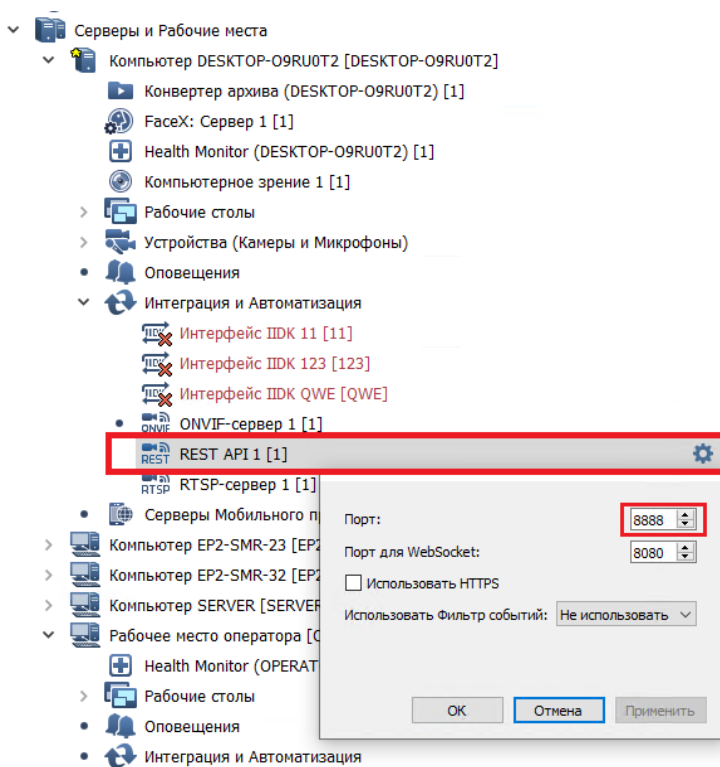


Рис. 7: Создание объекта REST API

Поле «Порт» будет использоваться в параметрах подключения к серверу «SecurOS FaceX». По умолчанию имеет значение 8888. Опция «Использовать HTTPS» должна быть выключена.

Внимание! Для работы с интеграционным интерфейсом RestAPI потребуется создать пользователя в системе и назначить ему права («корона») на объект RestAPI. Разделы 5.2.5 Пользователь и 5.2.7 Права пользователя документа SecurOS Administration Guide.pdf.

После проделанных операций в настройках объекта ПК сервера необходимо явно указать его IP-адрес (Рис. 8).

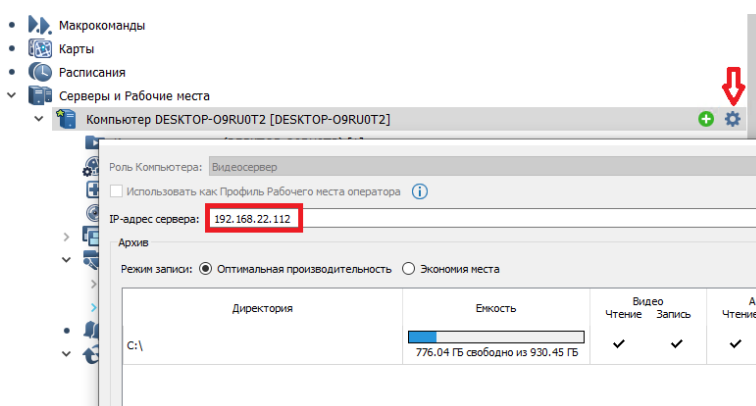


Рис. 8: Настройки компьютера сервера

Для получения более подробной информации по настройке объекта «FaceX: Сервер» обратитесь к документации по СБИ SecurOS FaceX.

3.2. Настройка драйвера

Перед началом работы с драйвером необходимо добавить его в разделе «Драйверы». Добавление драйверов в ПК «Бастион-3» описано в документе «Бастион-3. Руководство администратора».

Сначала следует выбрать пункт «Конфигуратор» для драйвера «Бастион-3 – SecurOS FaceX» в разделе драйверов «Панель управления» ПК «Бастион-3» (Рис. 9).

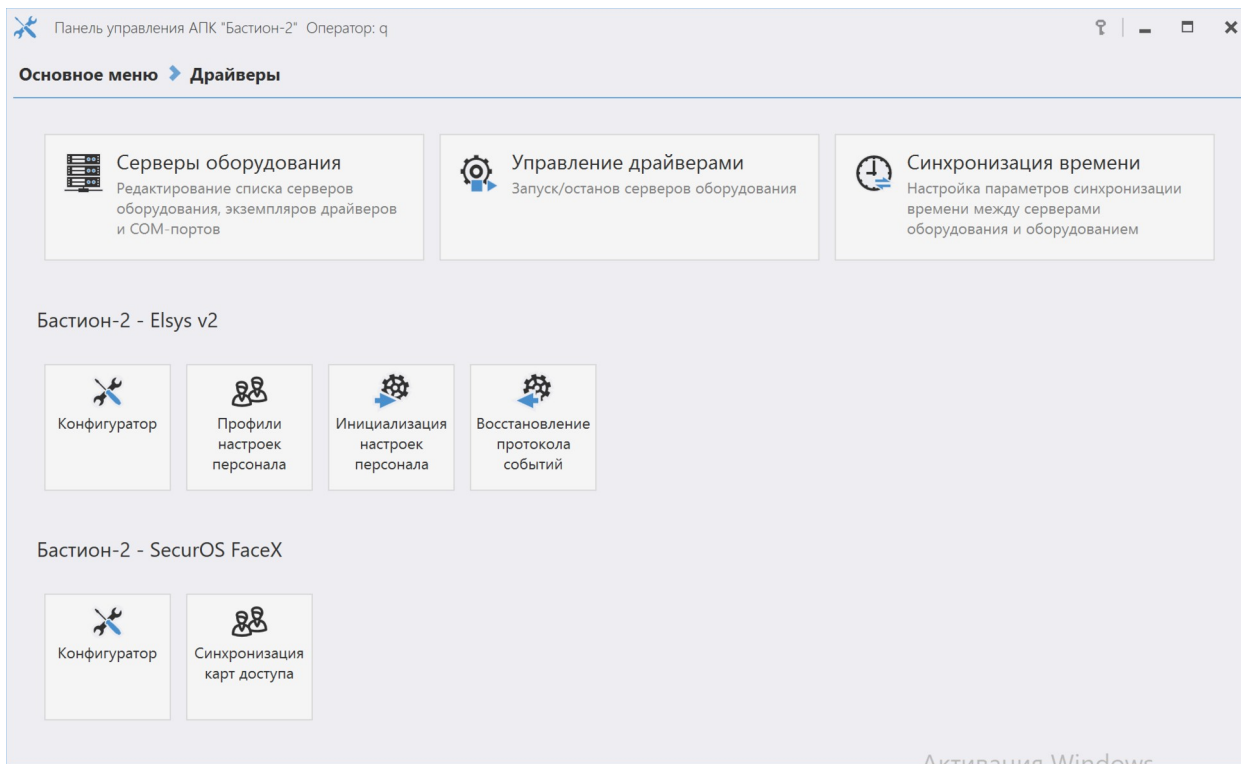


Рис. 9: Настройка драйвера «Бастион-3 – SecurOS FaceX»

Окно конфигуратора представлено на Рис. 10 и состоит из дерева конфигурации, панели инструментов и вкладки с информацией.

Для настройки модуля интеграции следует выполнить следующие действия:

1. Установить общие настройки работы системы.
2. Добавить и настроить соединения с серверами SecurOS FaceX.
3. Получить списки камер с серверов SecurOS FaceX и настроить для них режим работы.
4. Добавить для камер точки прохода и определить режимы доступа для них.
5. Добавить для камер необходимые виртуальные точки прохода и определить направления прохода.
6. Настроить СКУД для двухфакторной аутентификации, если этот режим доступа используется.

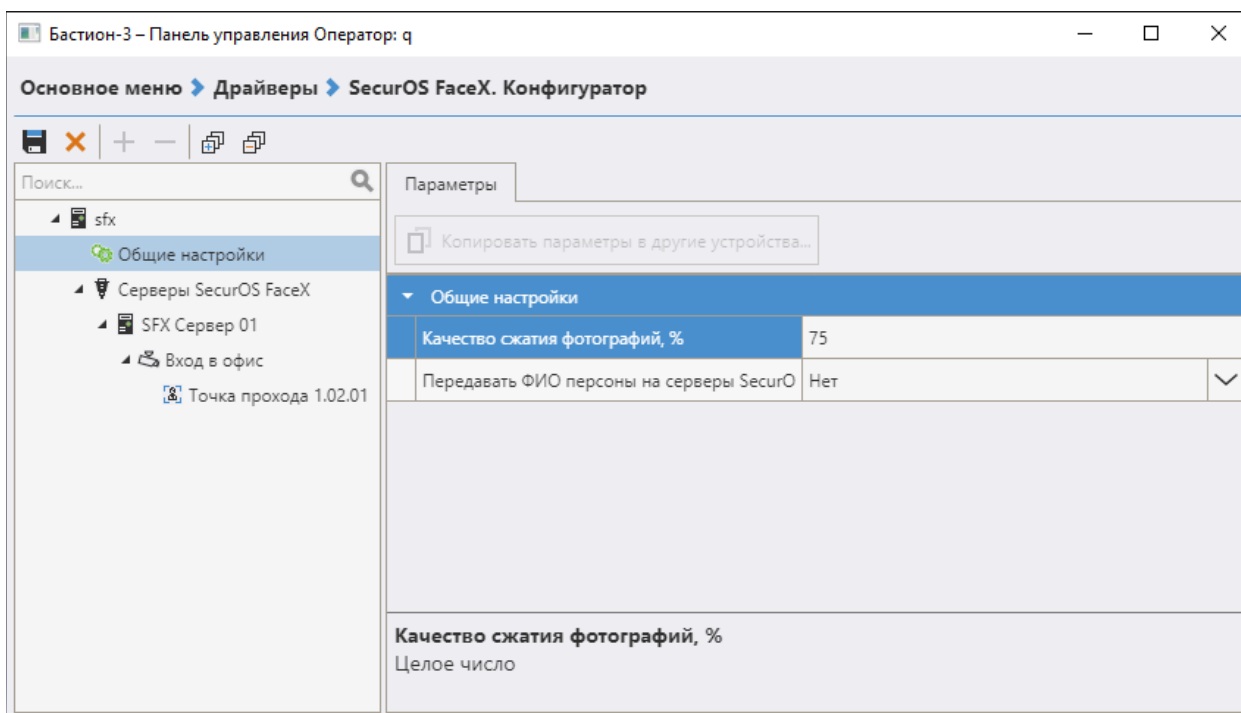


Рис. 10: Конфигуратор драйвера «Бастион-3 – SecurOS FaceX»

3.2.1. Основные настройки

В основных настройках определяются следующие параметры:



Качество фотографий, % – качество сжатия изображений с видеокамер, передаваемых с серверов «SecurOS FaceX» в ПК «Бастион-3» при событиях прохода. Следует иметь в виду, что эти фотографии используются для:

1. Отображения в расширенных сообщениях главного окна ПК «Бастион-3» при возникновении событий;
2. Сохранения в журнал событий ПК «Бастион-3» вместе с событиями.

Не рекомендуется выставлять положение ползунка близко к максимальному значению шкалы, так как это сильно увеличивает занимаемое изображениями место в БД.

Передавать ФИО персоны на сервера SecurOS – при установке этой опции на сервера SecurOS FaceX будет загружаться полная информация о владельце карты (ФИО, фотография, код карты). При выключенной настройке на сервер «SecurOS» передаются только код карты и фото персоны.

3.2.2. Настройка соединений с серверами SecurOS FaceX

В узел «Серверы SecurOS FaceX» добавляются серверы распознавания. Для добавления нового сервера следует нажать кнопку  «Добавить Сервер» на панели инструментов конфигуратора, для удаления – кнопку  «Удалить». Настройки подключения к серверу «SecurOS FaceX» представлены следующими параметрами (Рис. 11):

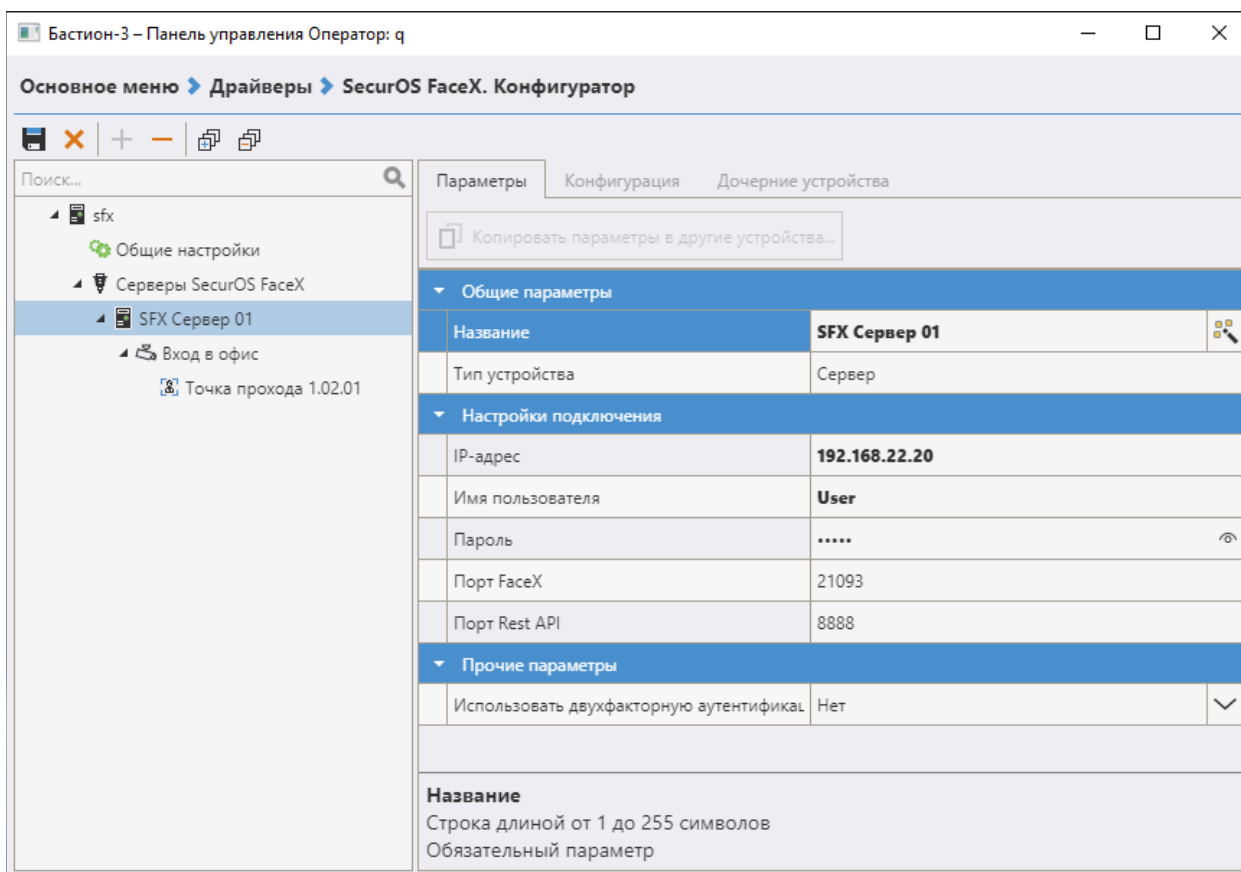


Рис. 11: Настройки подключения к серверу SecurOS FaceX

Название – произвольное текстовое название сервера.

IP-адрес – IP адрес сервера «SecurOS FaceX».

Имя пользователя – имя пользователя SecurOS для подключения к серверу.


Пароль – пароль указанного пользователя для подключения.


Порт FaceX – порт подключения к серверу «SecurOS FaceX» (значение по умолчанию 21093).

Порт RestApi – порт подключения к серверу «SecurOS» по REST API (значение по умолчанию 8888).

Использовать двухфакторную аутентификацию на сервере SecurOS FaceX – включение режима двухфакторной аутентификации на стороне драйвера.

Внимание! Для работы двухфакторной идентификации должны быть выполнены соответствующие настройки на сервере SecurOS FaceX (см. п. Настройка СБИ SecurOS FaceX).

После указания всех параметров подключения необходимо сохранить сделанные настройки . При этом автоматически будет установлено соединение с сервером.

При успешном соединении с сервером, для получения списка доступных камер распознавания лиц, необходимо перейти на вкладку «Конфигурация» и выполнить импорт списка, нажав на кнопку  Импорт... (Рис. 12).

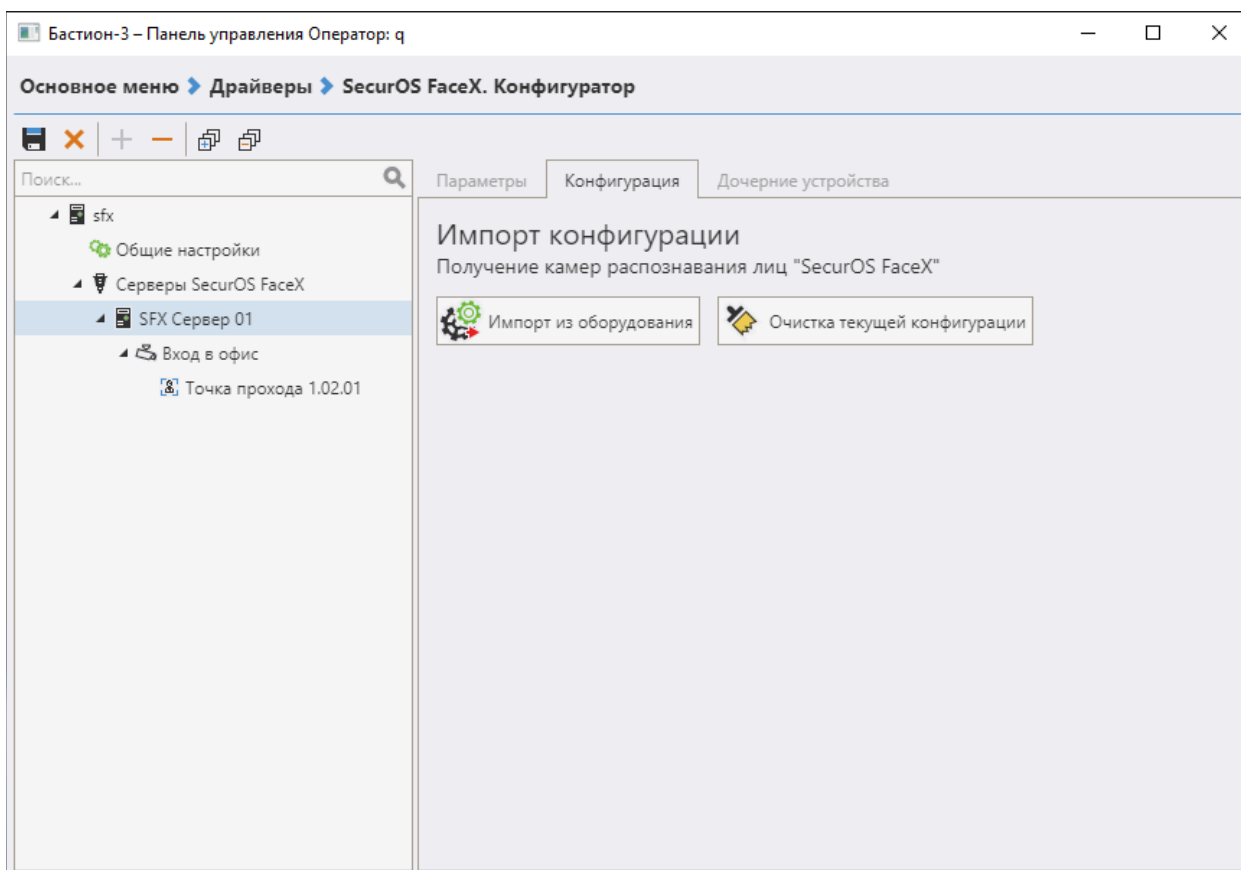


Рис. 12: Импорт списка камер распознавания лиц

При успешном чтении списка камер появится модальное окно выбора настроек импорта. Если отметить пункт «Заменять названия устройств», то ранее отредактированные названия камер заменятся на названия, полученные с сервера распознавания (Рис. 13).

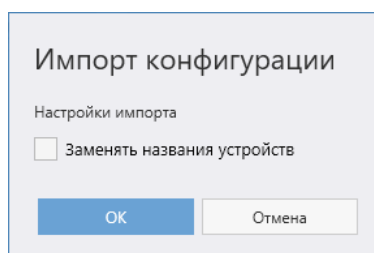



Рис. 13: Запрос замены
названия камер

По нажатию кнопки  **Очистка текущей конфигурации** выполняется очистка всех настроек выбранного сервера распознавания и удаление всех дочерних устройств.

3.2.3. Настройка работы с камерами

Полученные камеры распознавания лиц отображаются в дереве устройств как дочерние элементы серверов распознавания. Для настройки работы камеры в составе драйвера необходимо выбрать камеру в дереве устройств (Рис. 14).

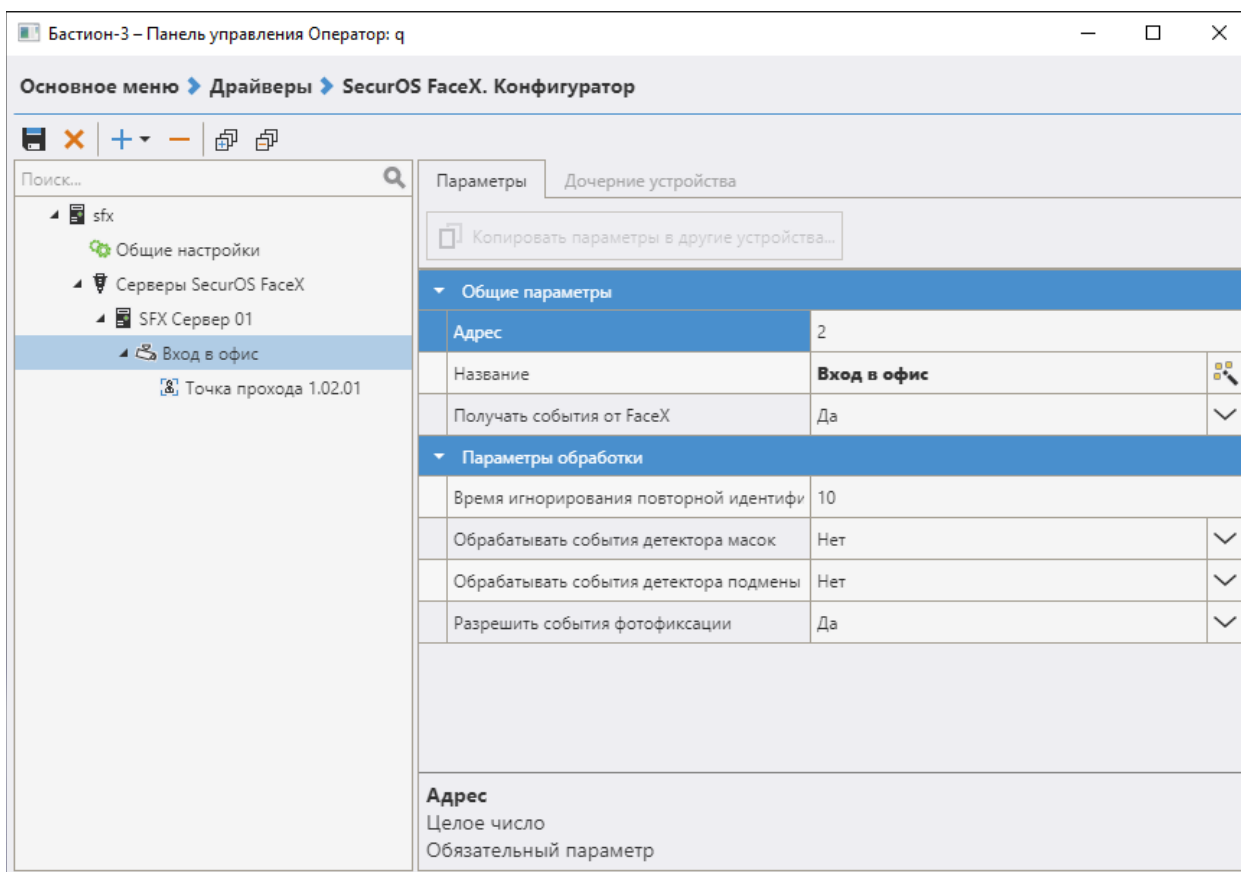


Рис. 14: Настройка параметров работы камеры распознавания лиц

Название – текстовое название камеры, полученное с сервера при импорте или автоматически созданное. Может быть изменено по усмотрению.

Получать события от FaceX – включение/отключение обработки событий от камеры. По умолчанию включена.

Время игнорирования повторной идентификации – параметр задает время, в течение которого повторное определение персоны в зоне обзора камеры будет проигнорировано.

Обрабатывать события детектора масок – при включении этой опции драйвер будет принимать событие о наличии маски на лице человека от сервера SecurOS FaceX. В случае, когда включена фотофиксация, драйвер будет генерировать события с припиской «Отсутствует маска!». Для режима идентификации и режима двухфакторной аутентификации детектор масок является дополнительным критерием прохода (Рис. 15).

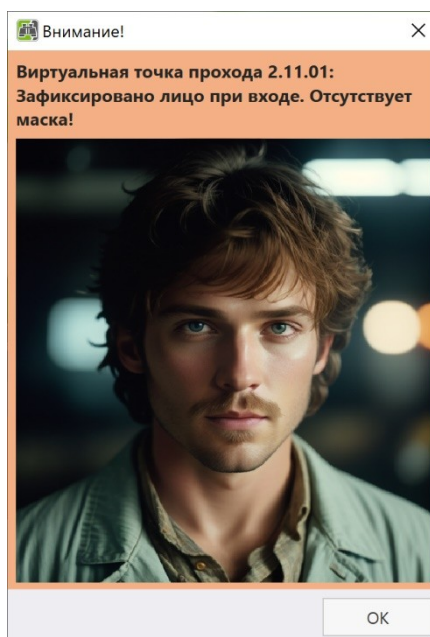


Рис. 15: Отказ доступа – отсутствие маски

Обрабатывать события детектора подмены лица – при включении этой опции драйвер будет принимать событие о возможной подмене лица. В случае, когда включена фотофиксация, драйвер будет генерировать события с припиской «Возможна подмена!». Для режима идентификации и режима двухфакторной аутентификации детектор подмены лица является дополнительным критерием прохода (Рис. 16).

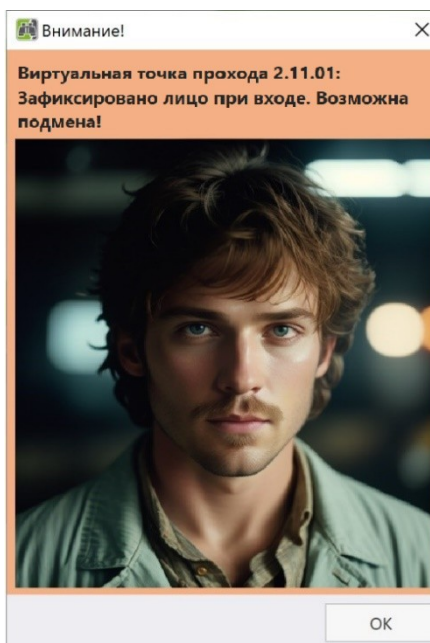


Рис. 16: Отказ доступа – возможна подмена лица


Внимание! Для получения событий детектора масок и детектора подмены лица на сервере SecurOS FaceX для выбранной камеры должны быть включены опции «Детекция масок» и «Защита от подмены лица» (см. п. Настройка СБИ SecurOS FaceX).

Разрешить событие фотофиксации – при отключении этой опции драйвер не будет генерировать события «Зафиксировано лицо» в любом из выбранных режимов при обнаружении лица.

Следует учитывать, что события обнаружения лица генерируются при появлении известных или неизвестных лиц в поле зрения камеры. Именно к этим событиям могут быть прикреплены фотографии с изображением распознанной персоны. В целях экономии места в БД можно отключить генерацию этих событий для отдельных точек прохода.

3.2.4. Точки прохода

К каждой камере распознавания можно привязать физическую и/или виртуальную точку прохода.

Для этого необходимо выбрать камеру в дереве устройств и нажать кнопку «Добавить»  или щелкнуть правой кнопкой мыши и выбрать тип добавляемой точки прохода (Рис. 17).

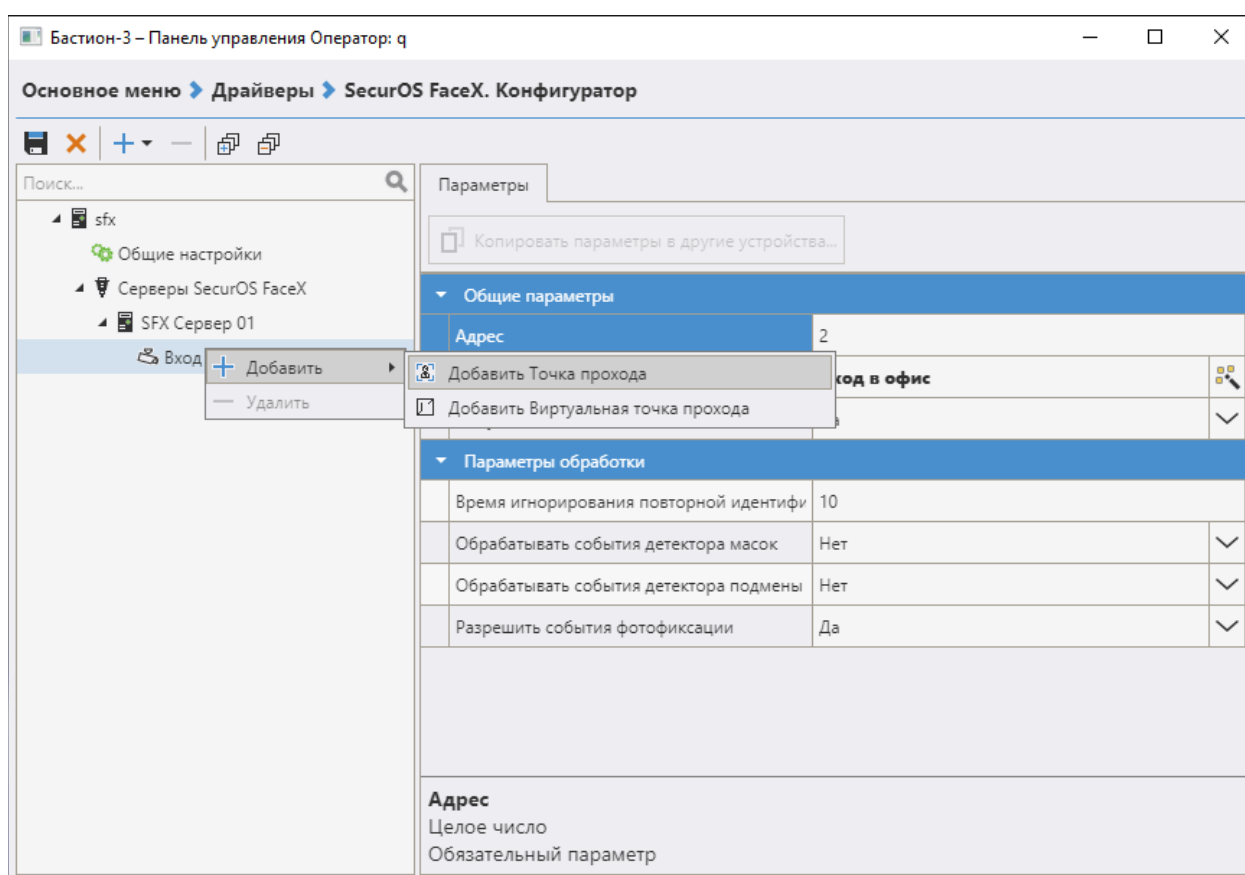


Рис. 17: Добавление точки прохода

3.2.4.1. Физические точки прохода

Выбрав при добавлении пункт «Точка прохода», будет осуществлена привязка камеры распознавания к считывателю физической точки прохода (двери, турникета, ворот). Настройки привязки и функционирования точки прохода имеют следующий вид (Рис. 18).

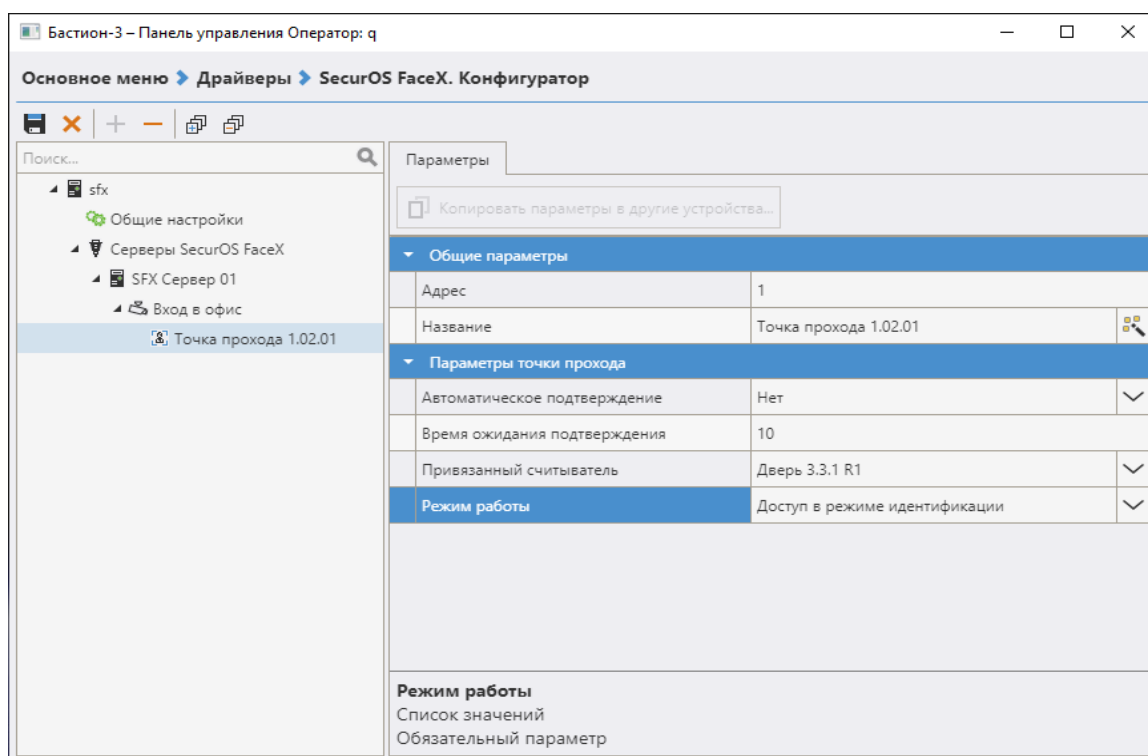


Рис. 18: Настройки работы физической точки прохода

Название – текстовое название точки прохода, связанной с камерой. Название будет фигурировать в событиях системы распознавания (но не СКУД). Может быть изменено по усмотрению.

Автоматическое подтверждение – опция необходима при временной неисправности сервера SecurOS FaceX, ее включение автоматически подтверждает доступ при использовании режима двухфакторной аутентификации.

Время ожидания подтверждения доступа – задает время ожидания подтверждения доступа персоны в режиме двухфакторной аутентификации (минимальное время 3 сек, максимальное 60 сек.).

Привязанный считыватель – считыватель точки прохода, на который будет передаваться код карты пользователя в режиме Идентификации или команды подтверждения в режиме Двухфакторной аутентификации.

Режим работы – определяет режим предоставления доступа для выбранного направления прохода. Доступны следующие варианты:

Доступ только по карте – в этом режиме точка прохода будет работать без использования биометрической идентификации. Этот режим можно выбирать, если необходимо временно отключить режим идентификации.

Доступ в режиме идентификации (по лицу или по карте) – в этом режиме доступ будет предоставляться либо при успешной идентификации по лицу (без прикладывания карты доступа), либо при предъявлении карты к считывателю. Этот режим выбирается по умолчанию.

Доступ в режиме двухфакторной аутентификации – в этом режиме при предъявлении карты к считывателю, драйвер SecurOS FaceX проверяет, было ли распознано лицо

владельца карты в пределах времени ожидания подтверждения доступа до или после предъявления карты. Если от сервера SecurOS FaceX приходит событие об идентификации посетителя, то драйвер выдает подтверждение/отказ в доступе.

3.2.4.2. Настройка СКУД для двухфакторной аутентификации

Для обеспечения работы считывателя совместно с СБИ в режиме двухфакторной аутентификации необходимо, чтобы в настройках оборудования СКУД Elsys (настройки в Автономном конфигураторе) для соответствующего считывателя была включена опция «Подтверждать доступ для карт с полномочиями "Доступ с подтверждением"» в блоке настроек «Полномочия дежурного оператора» (Рис. 19).

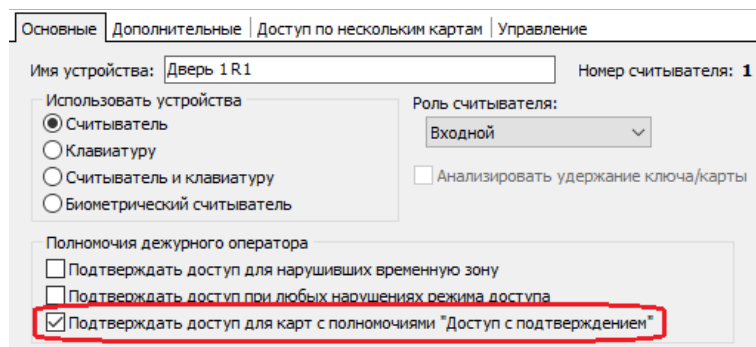


Рис. 19: Параметры считывателя в настройках СКУД Elsys

На вкладке «Дополнительные» необходимо включить опцию «Мониторинг предоставления доступа» (Рис. 20).

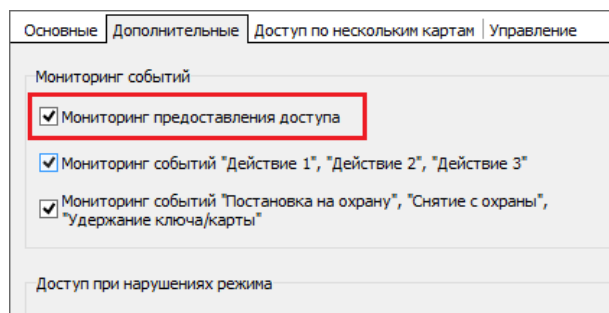


Рис. 20: Настройка мониторинга событий считывателя СКУД Elsys

Всем пропускам, которые должны иметь доступ на считывателях, работающих в режиме двухфакторной аутентификации, должен быть задан Профиль персонала, в настройках которого должен быть указаны полномочия «Доступ с подтверждением» (Рис. 21).

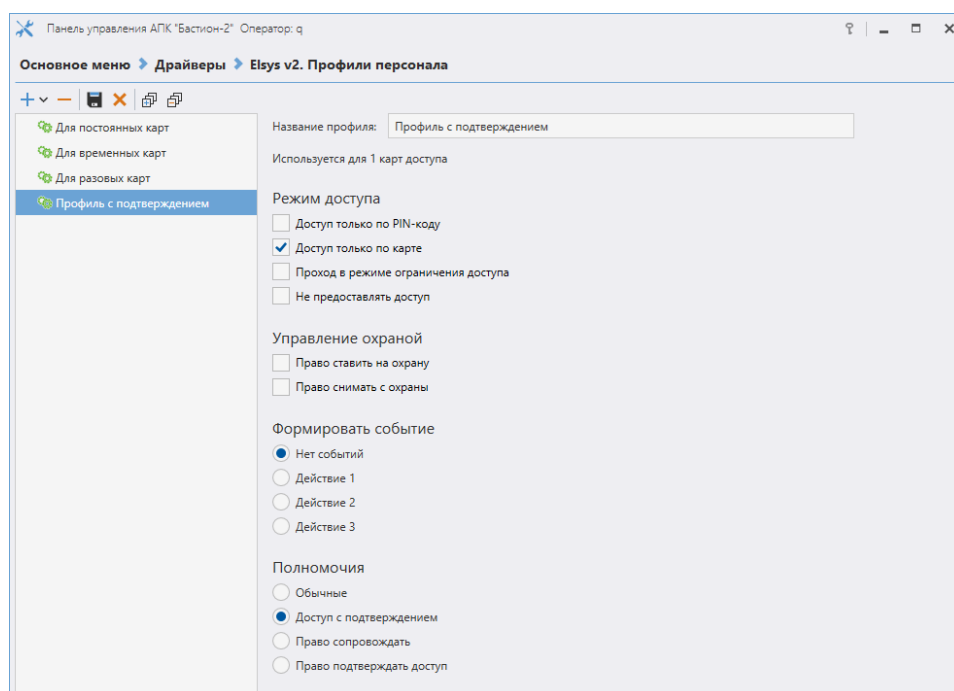


Рис. 21: Полномочия пропусков для доступа в режиме двухфакторной аутентификации

Для работы двухфакторной идентификации необходимо провести дополнительные настройки драйвера и сервера SecurOS FaceX:

- в настройках драйвера для выбранного в дереве устройств сервера распознавания установить пункт «Использовать многофакторную СКУД-аутентификацию на сервере SecurOS FaceX» (Рис. 11).
- в настройках сервера SecurOS FaceX дополнительно включить опцию «Многофакторная СКУД-аутентификация», настроить время ожидания верификации и порог подобия для режима СКУД.

3.2.4.3. Виртуальные точки прохода

Виртуальная точка прохода не связана с реальным преграждающим устройством, но позволяет отслеживать местоположение персонала и посетителей в зонах, контролируемых камерами видеонаблюдения, подключенными к серверам SecurOS FaceX.

Виртуальная точка прохода представляет из себя объект «Дверь» с привязанным к ней одним считывателем. Таким образом, виртуальные точки прохода можно использовать и в уровнях доступа (соответствующий считыватель), и в областях контроля (как дверь). Виртуальные точки прохода всегда являются односторонними (то есть, работают или на вход, или на выход).

Чтобы создать виртуальную точку прохода со считывателем необходимо выбрать камеру и при добавлении нового дочернего устройства выбрать пункт «Виртуальная точка прохода».

В настройках виртуальной точки прохода можно задать текстовое название. А в настройках виртуального считывателя – направление прохода, за которое он будет отвечать (Рис. 22).

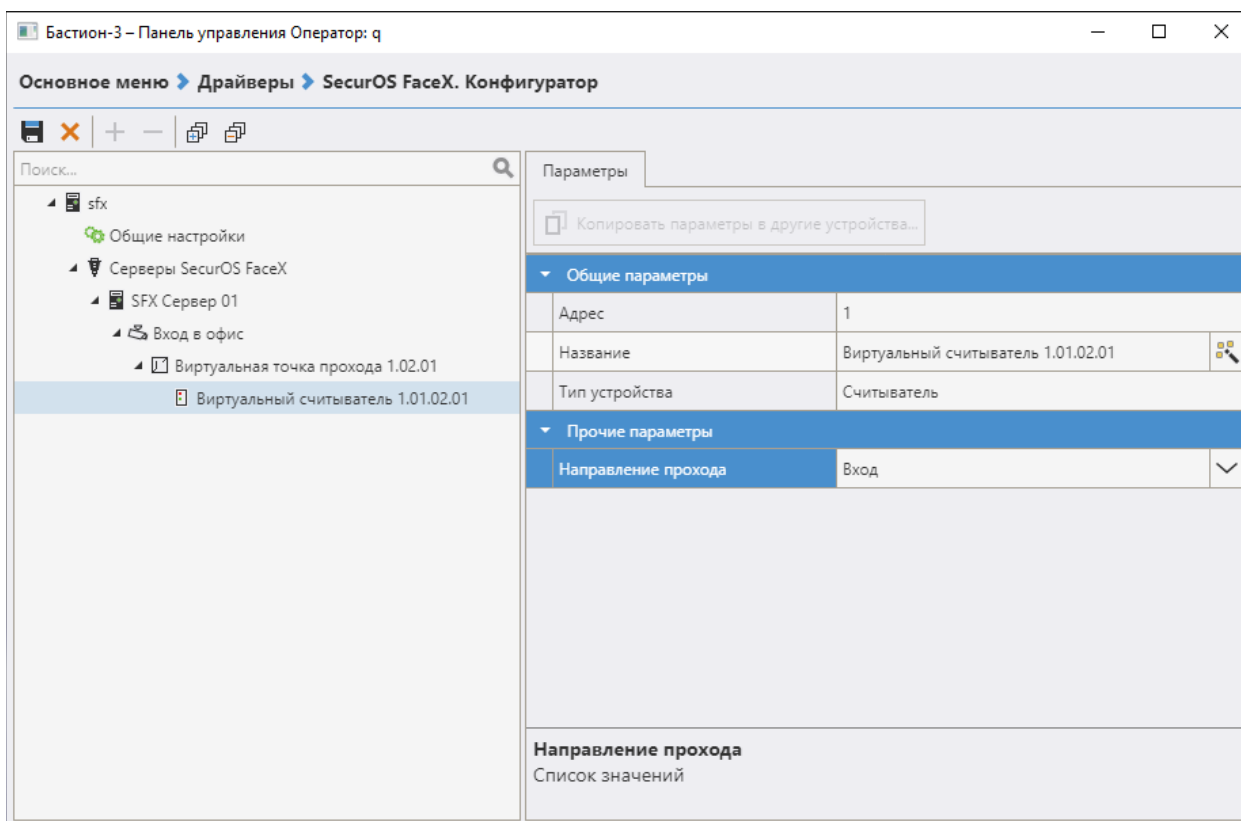


Рис. 22: Настройки виртуальной точки прохода

Название – текстовое название, присвоенное виртуальному считывателю.

Направление прохода – вход или выход. От направления прохода зависят связанные с виртуальной точкой события:

- Вход/выход в зону, возможна подмена
- Вход/выход из зоны
- Зафиксировано лицо при входе/выходе
- Зафиксировано лицо при входе/выходе (без маски)
- Зафиксировано лицо при входе/выходе. Возможна подмена!

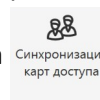
4. Работа в штатном режиме

4.1. Операции с пропусками

Все выдаваемые в системе пропуска с **фотографией** синхронизируются с серверами SecurOS FaceX в момент установки связи с ними.

При первичном запуске драйвера или при наличии не синхронизированных записей есть возможность запустить в ручном режиме процесс полной синхронизации карт доступа баз данных «Бастион-3» и SecurOS FaceX. Для этого необходимо запустить форму управления синхронизацией

при помощи кнопки в панели управления «Синхронизация карт доступа



» (Рис. 23).

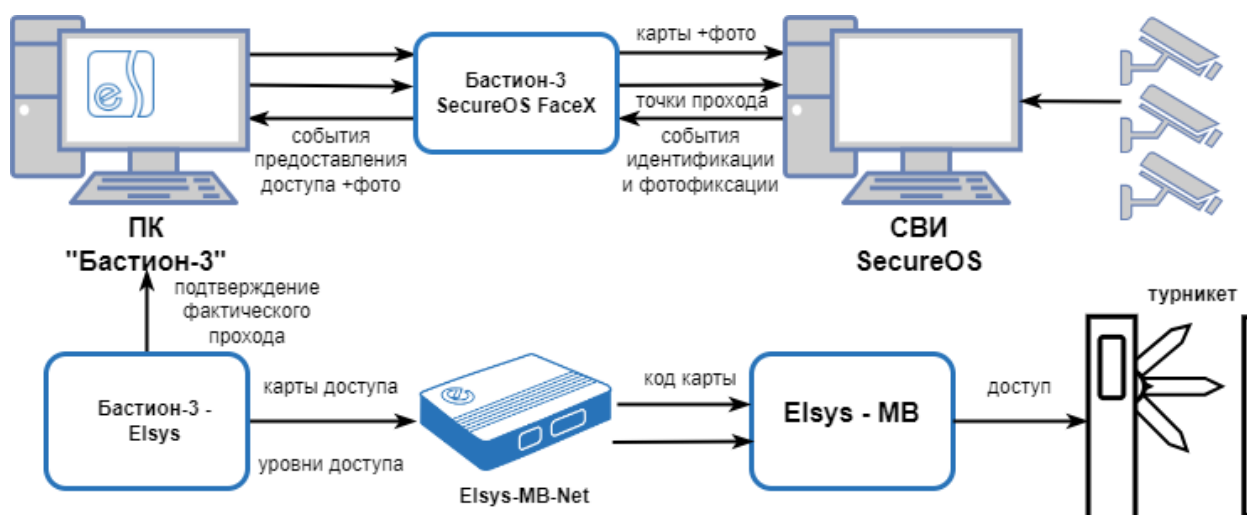


Рис. 24: Работа системы в режиме идентификации

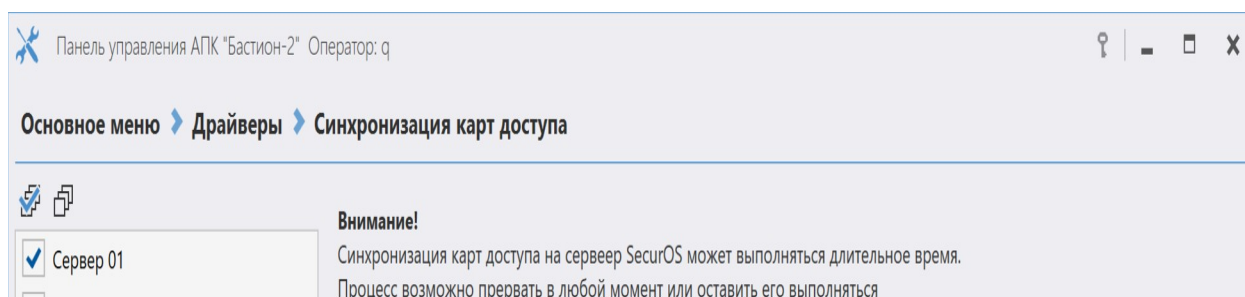


Рис. 23: Окно запуска синхронизации карт доступа

В списке серверов отображаются все серверы FaceX, при этом серверы, с которыми нет связи, неактивны и недоступны для выбора, а серверы, на которых уже идет фоновая синхронизация, имеют соответствующий статус и тоже недоступны для выбора.

При выборе серверов, на которых требуется произвести синхронизацию карт доступа, становится активна кнопка «Запустить синхронизацию».

Процесс в любой момент можно остановить или перевести в фоновый режим, нажав кнопку отмены и выбрав соответствующее действие в открывшемся диалоге.

Изменения при операциях с пропусками, включая изменения фотографий, автоматически передаются и записываются в SecurOS FaceX. Если по какой-то причине (некачественное фото, более одного лица на фото) пропуск не сохранился в SecurOS FaceX, будет выдано событие «<ФИО посетителя>: Не удалось синхронизировать пропуск с сервером SecurOS FaceX: <Текст ошибки>». При отсутствии фотографии в синхронизируемом пропуске будет выдано сообщение «<ФИО посетителя>: Пропуск без фотографии не будет загружен на сервер SecurOS FaceX».

Внимание! Если у персоны в БД есть несколько активных пропусков, то синхронизация выполнится только для первой записи, найденной в базе данных.

4.2. Режим идентификации

В режиме идентификации доступ посетителю может быть предоставлен либо при распознавании его лица, либо при предъявлении карты к считывателю (если считыватель установлен и активен). Для получения доступа на точке прохода посетителю достаточно встать напротив камеры видеонаблюдения. СБИ SecurOS FaceX проанализирует изображение лица посетителя, полученное с камеры, и сравнит его с фотографиями всех активных пропусков в системе (Рис. 24).

При появлении в поле зрения камеры лица в «Бастион-3» будет выдано событие **«<Название точки прохода>: Зафиксировано лицо при входе/выходе»** с привязанной фотографией посетителя, полученной с камеры видеонаблюдения, если генерация событий фотофиксации не отключена в настройках направления прохода (п. 3.2.3). При включенной обработке событий от детектора масок в случае, если на распознанном лице отсутствует маска, будут приходить события **«<Название точки прохода>: Зафиксировано лицо при входе/выходе. Отсутствует маска!»**. При включенной обработке событий от детектора подмены лица в случае, если обнаружена подмена лица будут приходить события **«<Название точки прохода>: Зафиксировано лицо при входе/выходе. Возможна подмена!»**.

Если сервер SecurOS FaceX обнаружит в системе активный пропуск, имеющий фотографию лица, совпадающего с лицом на изображении, полученного с камеры видеонаблюдения, то соответствующий код карты будет отправлен на контроллер СКУД ELSYS, а в «Бастион-3» будет выдано событие (с привязанным изображением лица посетителя, полученным с камеры видеонаблюдения) **«<Название точки прохода>: Успешная идентификация <ФИО посетителя>»**. При этом окончательное решение о допуске принимает СКУД ELSYS на основе имеющихся прав и уровней доступа.

При включенной обработке событий от детектора масок в случае, если на распознанном лице отсутствует маска, будут приходить события **«<Название точки прохода>: В доступе отказано <ФИО посетителя> - отсутствие маски на лице»**.

При включенной обработке событий от детектора подмены лица в случае, если обнаружена подмена лица будут приходить события **«<Название точки прохода>: В доступе отказано <ФИО посетителя> - возможна подмена!»**.

Во всех случаях фотография, прикреплённая к генерируемому событию, будет отображена в окне расширенного сообщения (если включена соответствующая настройка в параметрах «Бастион-3»).

4.3. Режим двухфакторной аутентификации

В режиме двухфакторной аутентификации посетитель прикладывает пропуск к считывателю. При этом его лицо должно быть в зоне обзора камеры видеонаблюдения, связанной с этим считывателем. Контроллер Elsys-MB проверяет права предъявленной карты доступа. Если для карты активна опция «Доступ с подтверждением», то контроллер выдает запрос внешней аутентификации карты, который получает модуль «Бастион-3 – SecurOS FaceX». Далее модуль ожидает от сервера SecurOS FaceX событие об идентификации или верификации, и, если идентифицированный посетитель соответствует владельцу приложенной к считывателю карты, результат аутентификации передается обратно через драйвер «Бастион-3 – Elsys» в контроллер как подтверждение доступа (Рис. 25).

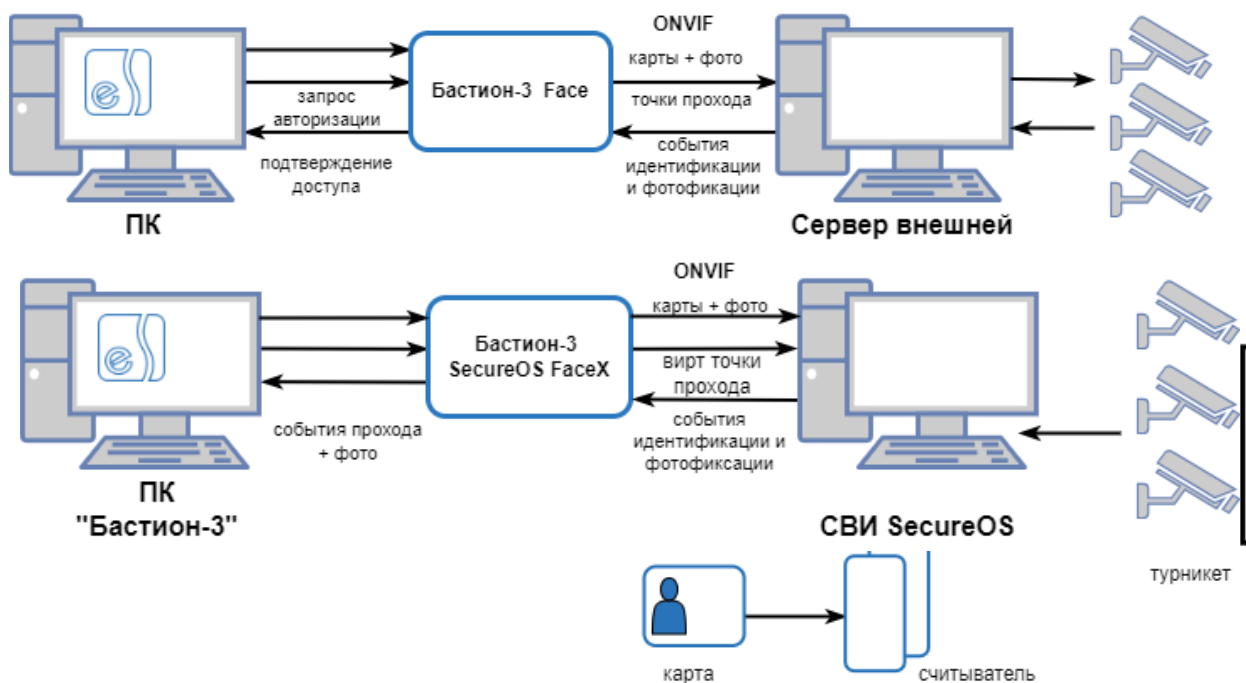


Рис. 25: Работа системы в режиме двухфакторной аутентификации

При появлении в поле зрения камеры лица, в ПК «Бастион-3» будет выдано событие «**<Название точки прохода>: зафиксировано лицо**», если генерация событий фотофиксации не отключена в настройках точки прохода.

Обнаружение маски и подмены лица осуществляется аналогичным идентификации образом.

Если личность посетителя была подтверждена по его изображению, то доступ будет предоставлен. В ПК «Бастион-3» будет выдано событие «**<Название точки прохода>: Успешная верификация <ФИО посетителя>**».

Если в течение заданного времени ожидания сервером SecurOS FaceX не будет зафиксировано лица владельца приложенной карты, то в ПК «Бастион-3» будет выдано тревожное событие «**<Название точки прохода>: отказ в доступе на вход/выход оператором <ФИО посетителя>**».

К событиям «зафиксировано лицо» и «доступ подтвержден» прикрепляется фотография посетителя, полученная с камеры видеонаблюдения. Если соответствующая настройка включена в параметрах «Бастион-3», то фотография будет отображена в окне расширенного сообщения.

Внимание! Режим двухфакторной аутентификации требует наличия связи и работоспособности не только контроллеров ELSYS, но и модулей ПК «Бастион-3» и серверов SecurOS FaceX. В случае неисправности хотя бы одного из компонентов, подтверждение доступа для карт передаваться не будет и в доступе будет отказано. В случае неисправности серверов SecurOS FaceX рекомендуется для соответствующих точек прохода устанавливать опцию «Автоматическое подтверждение».

4.4. Отслеживание прохода на виртуальных точках доступа

Для виртуальной точки прохода система SecurOS FaceX будет генерировать событие «**Зафиксировано лицо при входе/выходе**» с привязанным изображением лица посетителя, полученным с камеры видеонаблюдения (Рис. 26).



Если SecurOS FaceX обнаружит в системе активный пропуск, имеющий фотографию лица, совпадающего с лицом на изображении, полученного с камеры видеонаблюдения, то в ПК «Бастиян-3» будет выдано событие **«Идентификация при входе/выходе <ФИО посетителя>»**, и после проверки полномочий в ПК «Бастиян-3» соответствующие сообщения о штатном проходе **«Штатный вход/выход <ФИО посетителя>»** или наличие ограничений доступа **«Вход/выход запрещен <ФИО посетителя>»**.

При включенной опции обнаружения маски, и при её не обнаружении, для известной персоны будет выдано событие **«Идентификация при входе/выходе <ФИО посетителя>. Отсутствует маска!»**, и после проверки полномочий в ПК «Бастиян-3» соответствующие сообщения о штатном проходе **«Штатный вход/выход <ФИО посетителя> Отсутствует маска!»** или наличие ограничений доступа **«Вход/выход запрещен <ФИО посетителя> Отсутствует маска!»**.

При включенной опции обнаружения подмены лица, и при обнаружении попытки подмены, для известной персоны будет выдано событие **«Идентификация при входе/выходе <ФИО посетителя>. Возможна подмена!»**, и после проверки полномочий в ПК «Бастиян-3» соответствующие сообщения о штатном проходе **«Штатный вход/выход <ФИО посетителя> Возможна подмена!»** или наличие ограничений доступа **«Вход/выход запрещен <ФИО посетителя> Возможна подмена!»**.

Если соответствующая настройка включена в параметрах ПК «Бастиян-3», то фотография, прикрепляемая к событиям, будет отображена в окне расширенного сообщения.

5. Нештатные ситуации

Если после настройки подключения к серверу SecurOS FaceX соединение с сервером не устанавливается необходимо выполнить следующие проверки:

- проверить, что в настройках драйвера указан верный IP-адрес сервера. При этом указывать localhost или 127.0.0.1 при развернутом сервере SecurOS FaceX на том же ПК недопустимо. Требуется явное указание IP-адреса сетевого интерфейса с приоритетной метрикой!
- проверить, что порты FaceX и Rest API в настройках драйвера и SecurOS FaceX совпадают.
- проверить, не заняты ли указанные порты FaceX и Rest API другими приложениями. Как вариант, можно попробовать заменить вышеперечисленные порты на неиспользуемые.

Если подключение происходит, но список доступных камер распознавания недоступен или пустой требуется проверить корректность указания в настройках драйвера IP-адрес сервера SecurOS FaceX. Указывать localhost или 127.0.0.1 при развернутом сервере SecurOS FaceX на том же ПК недопустимо.

В случае потери связи с сервером «SecurOS FaceX» в «Бастиян-3» будет выдано событие **«Потеряно соединение с сервером SecurOS FaceX»**. При восстановлении связи будет выдано событие **«Установлено соединение с сервером SecurOS FaceX»**.

Режим двухфакторной аутентификации требует наличия связи и работоспособности не только контроллеров ELSYS, но и модулей ПК «Бастиян-3» и серверов «SecurOS FaceX». В случае



неисправности хотя бы одного из компонентов, подтверждение доступа для карт передаваться не будет и в доступе будет отказано. В случае неисправности серверов «SecurOS FaceX» рекомендуется для соответствующих точек прохода временно установить опцию «Автоматическое подтверждение».

6. Приложения

Приложение 1. История изменений

1.0.1 (15.11.2023)

[+] Первая версия, включена в комплект поставки ПК «Бастيون-3».