



Бастион-2 – SecurOS FaceX. Руководство
администратора

Версия 1.0.5

(17.10.2024)



Самара, 2024



Оглавление

1	Общие сведения.....	2
1.1	Назначение и область применения.....	2
2	Условия применения	2
2.1	Требования к совместимости	2
2.2	Лицензирование системы	3
3	Установка системы.....	3
4	Настройка системы	3
4.1	Настройка СБИ SecurOS FaceX	3
4.2	Настройка драйвера	7
4.2.1	Основные настройки	8
4.2.2	Настройка соединений с серверами SecurOS FaceX.....	8
4.2.3	Направления прохода	9
4.2.4	Настройка СКУД для двухфакторной аутентификации	12
4.2.5	Виртуальные точки прохода	14
5	Работа в штатном режиме.....	15
5.1	Операции с пропусками	15
5.2	Режим двухфакторной аутентификации.....	16
5.3	Режим идентификации.....	17
5.4	Отслеживание прохода на виртуальных точках доступа	18
6	Нештатные ситуации.....	18
	Приложения	20
	Приложение 1. История изменений.....	20

1 Общие сведения

1.1 Назначение и область применения

Модуль «Бастион-2 – SecurOS FaceX» предназначен для подключения к АПК «Бастион-2» системы 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 видеофиксации с его фотографией, сохранённой в АПК «Бастион-2».

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 типов (постоянные, временные и разовые).

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 видеофиксации, подключенных к серверу SecurOS FaceX.

2 Условия применения

2.1 Требования к совместимости

На модуль «Бастион-2 – SecurOS FaceX» распространяются те же требования к аппаратной и программной платформе, что и для АПК «Бастион-2».

Для работы с реальными точками прохода требуется наличие СКУД ELSYS и драйвера «Бастион-2 – ELSYS». Доступ в режиме идентификации (только по изображению лица с камеры) можно настроить только для точек прохода контроллеров ELSYS, которые подключены через коммуникационные сетевые контроллеры (КСК ELSYS MB-NET), для этого в сети должен быть доступен обмен информацией по портам 4001, 4002, 4003, 4096, 63000, 5433 (сетевые порты должны быть открыты). Другие варианты подключения могут использоваться только для режима двухфакторной аутентификации.

Для работы доступа в режиме идентификации версия прошивки КСК 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 — 10.7 и выше. Обмен данными между модулем «Бастион-2 – SecurOS FaceX» и СБИ SecurOS FaceX выполняется по протоколу HTTP.

Модуль совместим с АПК «Бастион-2» версии 2.1.1 и выше. Для работы модуля необходимо иметь установленную версию .Net Framework 4.7.2 или выше. Операционные системы Windows XP, Windows 7, Windows Server 2008, Windows Vista не поддерживаются ввиду отсутствия реализации технологии Web Socket. Рекомендуемая ОС – Windows 10.

2.2 Лицензирование системы

Для работы модуля требуется дополнительная 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-2 – SecurOS FaceX Исп. 1». Число необходимых лицензий не зависит от числа используемых видеокамер.

3 Установка системы

Для работы системы необходимо установить драйвер «Бастион-2 – SecurOS FaceX». Модуль может устанавливаться как в составе АПК «Бастион-2», так и отдельно от него, путем запуска файла инсталлятора SecurOsFaceXSetup.msi.

4 Настройка системы

4.1 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 направлениям прохода СКУД и виртуальным точкам прохода в конфигурации драйвера «Бастион-2 – SecurOS FaceX» (пп. 4.3.3 и 4.3.5).

На сервере SecurOS должен быть создан пользователь:

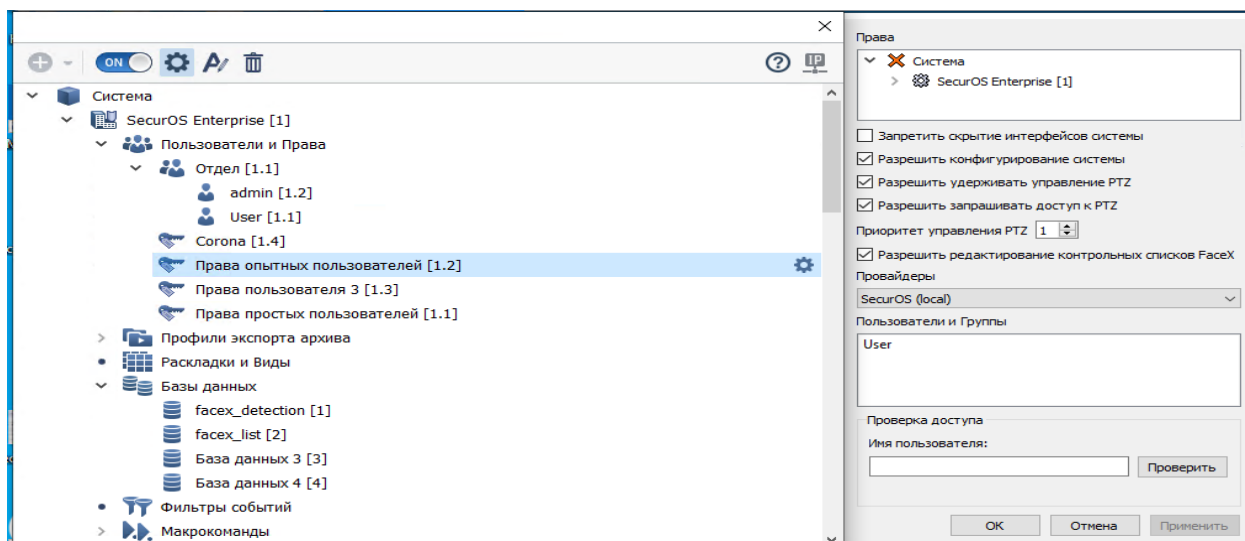


Рис. 1. Пользователь с правами на сервере SecurOS

Для работы модуля необходимо, чтобы на сервере «FaceX» были созданы и настроены БД детекций (facex_detect) и БД контрольных списков (facex_list). Необходимо указать ip-адрес сервера, порт и пароль. Значения по умолчанию: пароль — postgres, порт - 5432 (Рис. 2).

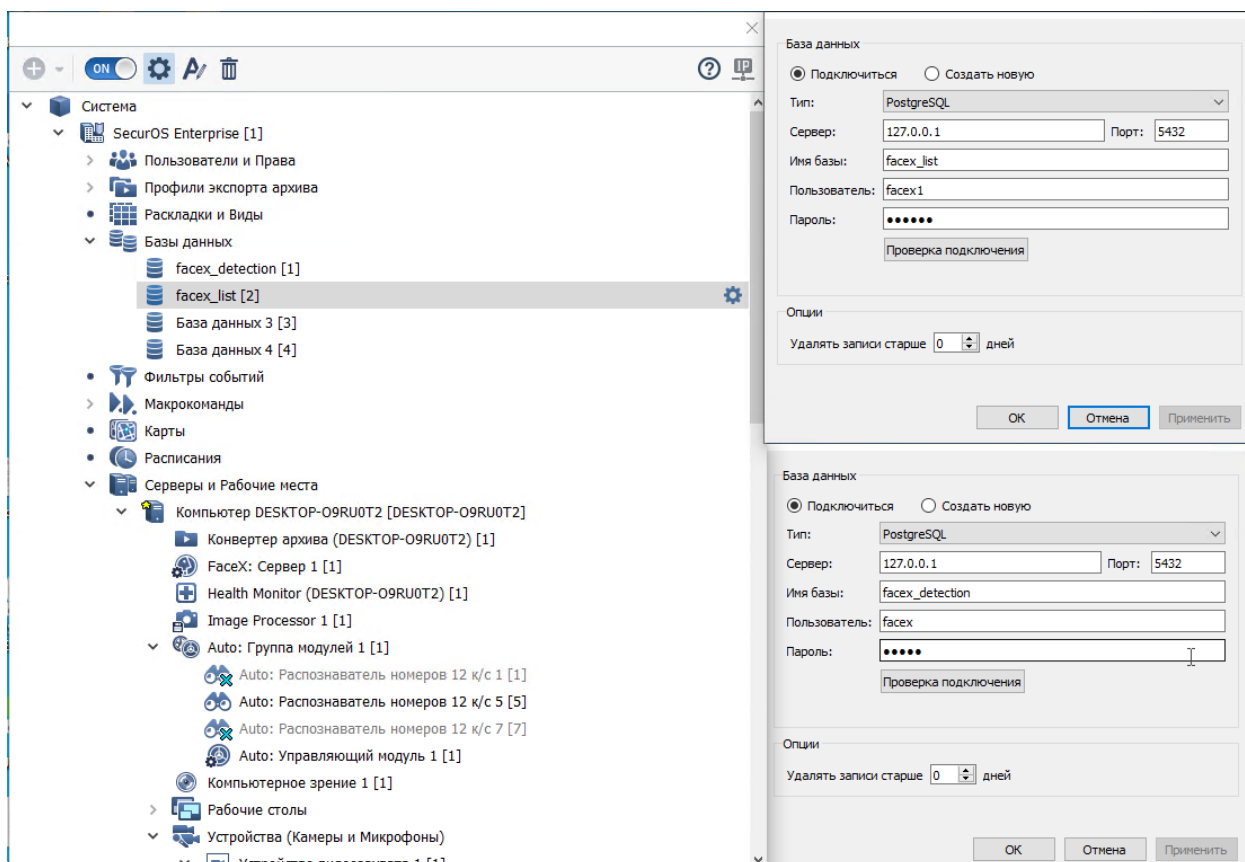


Рис. 2. Создание БД «детекций» и БД «контрольных списков»

В СБИ SecurOS FaceX должен быть создан объект «Face X: Сервер» (см. Рис. 3).

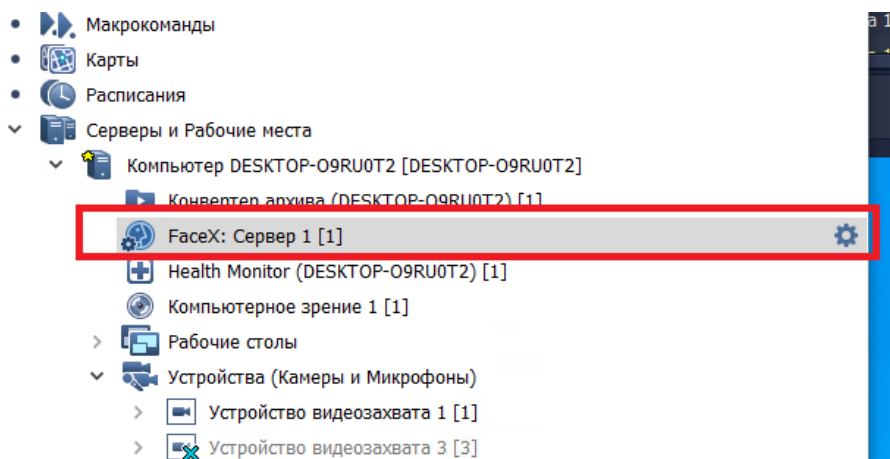


Рис. 3. Создание объекта «FaceX: Сервер»

Для настройки созданного объекта необходимо открыть меню настроек (Рис. 4).

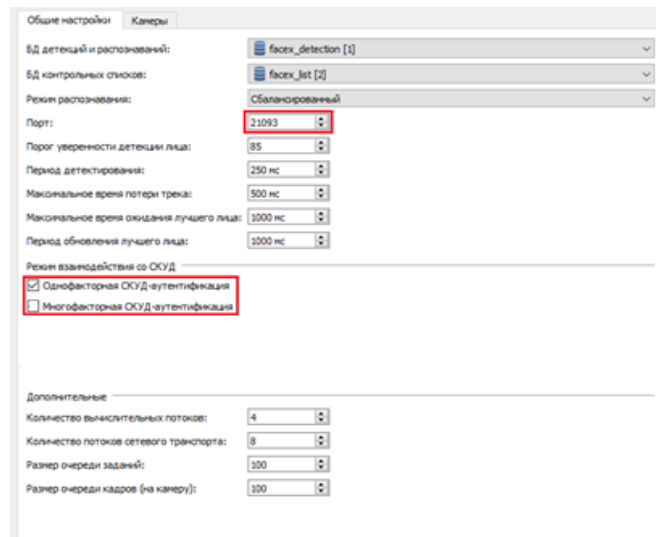


Рис. 4. Общие настройки объекта «FaceX: Сервер»

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

В режиме взаимодействия со СКУД необходимо выбрать «Однофакторная СКУД-аутентификация» для режимов идентификации (проход только по лицу) и двухфакторной аутентификации, когда сначала считывается карта, а потом проверяется лицо.

Режим «Многофакторная СКУД-аутентификация» следует выбирать только, если используется режим двухфакторной аутентификации, когда распознаётся лицо, а потом считывается карта.

Далее необходимо перейти на страницу «Камеры» (Рис. 5).

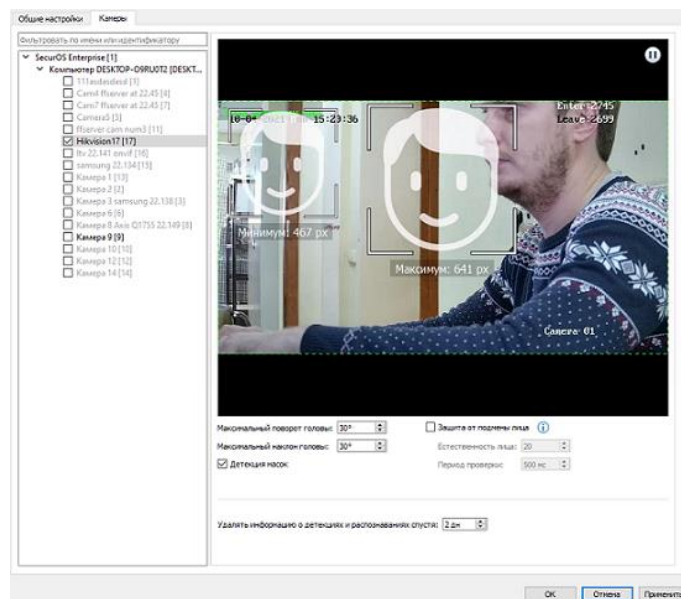


Рис. 5. Выбор списка камер для объекта «FaceX: Сервер»

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 персоналу, у которых параметр «Естественность лица», полученный входе распознавания, меньше установленного значения на сервере.

Далее на сервере SecurOS необходимо создать объект REST API (Рис. 6).

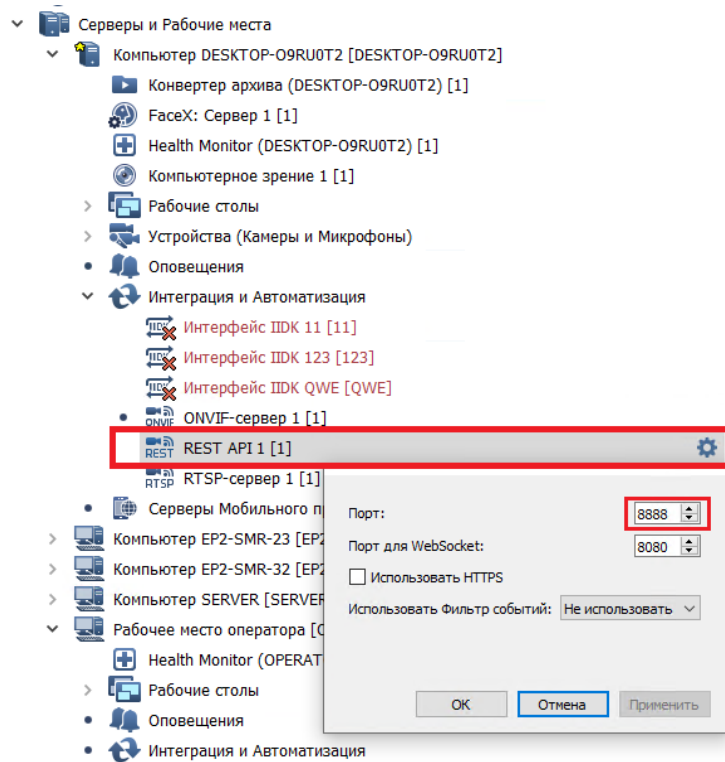


Рис. 6. Создание объекта REST API

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 назначит 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. 7).

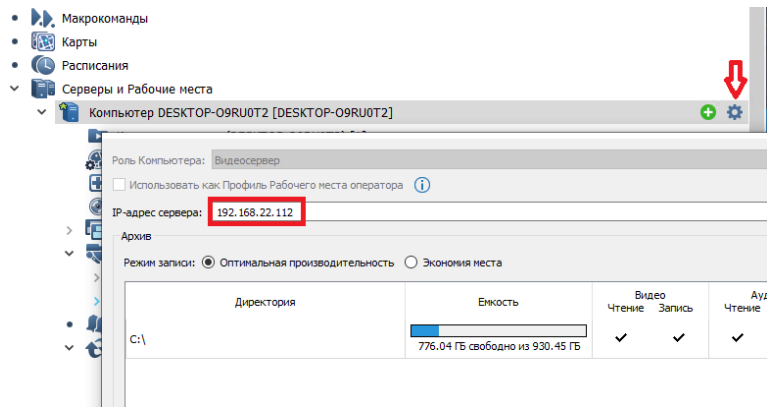


Рис. 7. Настройки компьютера сервера

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

4.2 Настройка драйвера

Для запуска драйвера следует добавить его экземпляр в конфигурацию АПК «Бастион-2». Добавление драйверов АПК «Бастион-2» описано в документе «Бастион-2. Руководство администратора».

Настройка драйвера осуществляется при помощи специального конфигуратора. Для его запуска следует нажать на кнопку «Конфигурация», располагающуюся в блоке драйвера «Бастион-2 – SecurOS FaceX» на вкладке «Драйверы» (Рис. 8).

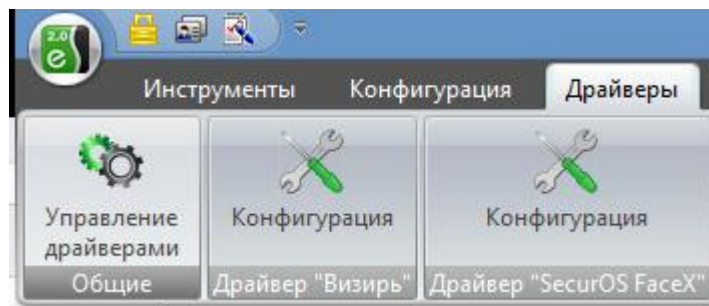






Рис. 8. Кнопка вызова конфигуратора драйвера «Бастион-2 – SecurOS FaceX»

Окно конфигуратора представлено на Рис. 9 и состоит из дерева конфигурации, панели инструментов и вкладки с информацией. Панель инструментов содержит кнопки: «Добавить» , «Удалить» , «Сохранить»  и «Отменить изменения» .

Для настройки модуля интеграции следует выполнить следующие действия:

1. Установить основные настройки работы системы;
2. Настроить соединения с серверами SecurOS FaceX;
3. Добавить направления прохода, определить режимы доступа для них и привязать к ним камеры;
4. Добавить необходимые виртуальные точки прохода и привязать к ним камеры;
5. Настроить СКУД для двухфакторной аутентификации, если этот режим доступа используется.

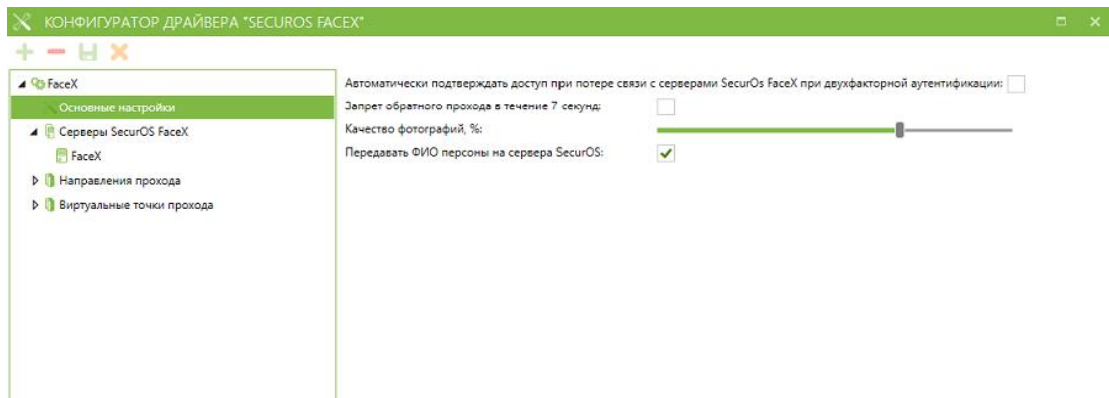


Рис. 9. Конфигуратор драйвера «Бастион-2 – SecurOS FaceX»

4.2.1 Основные настройки

В основных настройках определяются следующие параметры:

Автоматически подтверждать доступ при потере связи с серверами SecurOS FaceX при двухфакторной аутентификации (включено по умолчанию) – при включенной настройке, в случае потери связи драйвера «Бастион-2 – SecurOS FaceX» с серверами «SecurOS FaceX», драйвер будет выдавать автоматическое подтверждение доступа для всех карт, по которым такое подтверждение будет запрошено. Если настройка отключена, то при отсутствии связи с серверами «SecurOS FaceX» доступ в режиме двухфакторной аутентификации предоставляться не будет.

Запрет обратного прохода в течение 7 секунд – при включении этой опции доступ в режиме идентификации (доступа по лицу) не будет предоставляться, если посетитель попытается пройти в обратном направлении через двустороннюю дверь, ворота или турникет в течение 7 секунд после прохода.

Качество фотографий, % – качество сжатия изображений с видеокамер, передаваемых с серверов «SecurOS FaceX» в АПК «Бастион-2» при событиях прохода. Следует иметь в виду, что эти фотографии используются для:

1. Отображения в расширенных сообщениях главного окна АПК «Бастион-2» при возникновении событий;
2. Сохранения в журнал событий АПК «Бастион-2» 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.

4.2.2 Настройка соединений с серверами SecurOS FaceX

Узел «Серверы SecurOS FaceX» содержит подключения к серверам «SecurOS FaceX». Для добавления нового подключения следует нажать кнопку «Добавить» на панели инструментов конфигуратора, для удаления – кнопку «Удалить». Настройки подключения к серверу «SecurOS FaceX» представлены следующими параметрами (Рис. 10):

Имя сервера – произвольное текстовое название сервера.

Адрес сервера – IP адрес сервера «SecurOS FaceX».

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).

Логин – имя пользователя для подключения.

Пароль – пароль указанного пользователя для подключения.

Использовать многофакторную СКУД-аутентификацию на сервере SecurOS FaceX – настройка исключительно для режима двухфакторной аутентификации, в случае последовательности прохода «сначала лицо потом карта». Эта настройка позволяет использовать временный буфер распознанных лиц на сервере SecurOS FaceX.

Панель настроек подключения к серверу позволяет выполнить проверку правильности введенных данных и доступность самого сервера с помощью кнопки **«Проверить соединение с сервером»**. Результатом нажатия на кнопку будет либо надпись «ОК», если связь с сервером удалось установить, либо текст ошибки соединения.

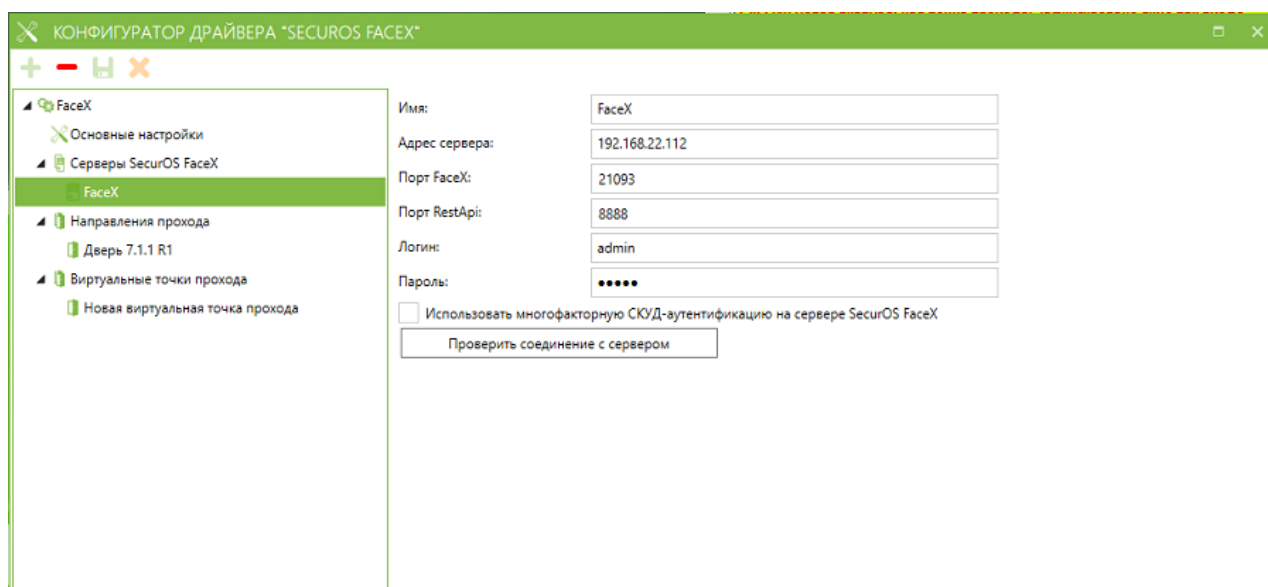


Рис. 10. Настройки подключения к серверу SecurOS FaceX

4.2.3 Направления прохода

Узел конфигурации «Направления прохода» содержит считыватели СКУД, подключенные к СБИ. Для подключения считывателей следует выделить узел настроек «Направления прохода» и нажать кнопку «Добавить» на панели инструментов, в результате чего откроется окно добавления направлений прохода (Рис. 11). Для исключения считывателя из СБИ следует выделить его в дереве конфигурации и нажать кнопку «Удалить». При сохранении настроек есть возможность удалить считыватели без привязанной камеры.

В рамках драйвера «Бастион-2 – SecurOS FaceX» каждому направлению прохода соответствует считыватель СКУД ELSYS.

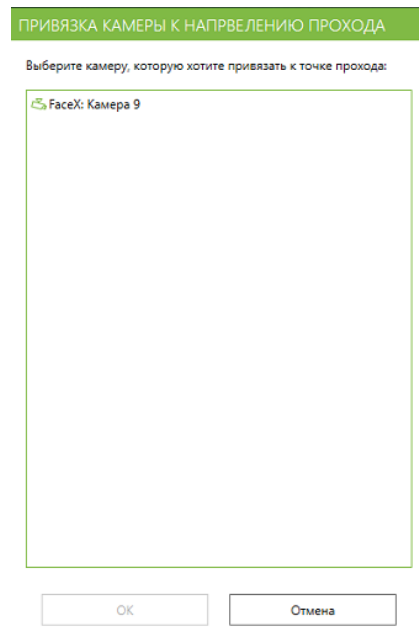


Рис. 11. Добавление считывателей

Настройки подключенных считывателей (Рис. 12) представлены параметрами, которые описаны ниже.

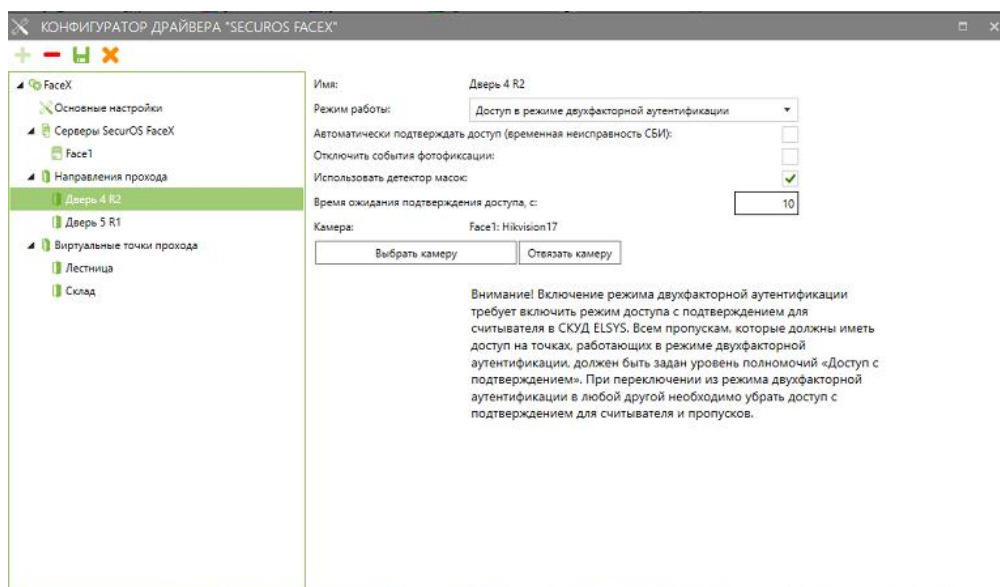


Рис. 12. Параметры направления прохода

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 – этом режиме посетитель сначала прикладывает карту к считывателю, затем модуль «Бастион-2 – SecurOS FaceX» дожидается от сервера « SecurOS FaceX» события об идентификации посетителя и выдает подтверждение / отказ в доступе.

Отключить события фотофиксации – при включении этой опции драйвер не будет генерировать события «Зафиксировано лицо» в любом из выбранных режимов.

Автоматически подтверждать доступ – опция необходима при временной неисправности сервера SecurOSFaceX, ее включение автоматически подтверждает доступ при использовании режима двухфакторной аутентификации.

Использовать детектор 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 «Зафиксировано лицо (в маске)» и «Зафиксировано лицо (без маски)». Для режима идентификации и режима двухфакторной аутентификации детектор масок является дополнительным критерием прохода Рис.13.

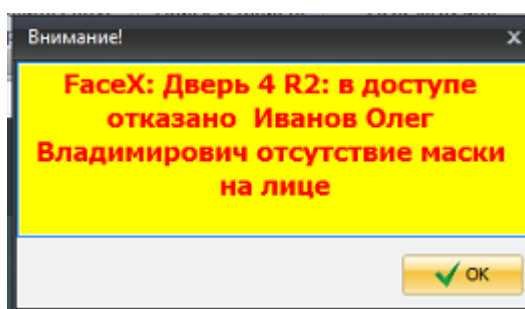


Рис.13. Отказ доступа – отсутствие маски

Для включения этой опции на сервере SecurOSFaceX необходимо включить опцию «Детекция масок» (Рис. 5).

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.

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

Камера – привязанная к направлению прохода камера сервера SecurOS FaceX. Имеется возможность отвязать привязанную камеру с помощью кнопки «Отвязать камеру» или привязать камеру с помощью кнопки «Выбрать камеру» с последующим выбором нужной камеры из списка доступных (см. Рис. 13). Также, если привязать уже используемую камеру к новому направлению прохода, то камера автоматически отвязается от предыдущего. Если пользователь не привяжет к направлению прохода камеру, то при сохранении конфигурации выдается запрос на удаление не привязанных направлений. Для отображения доступных на серверах SecurOS FaceX камер необходимо, чтобы были правильно настроены подключения к серверам SecurOS FaceX, а сами сервера были запущены и доступны для подключения.

Названия камер в списке формируются по следующему шаблону: <имя сервера SecurOS FaceX, на котором настроено подключение к камере>: <имя камеры на сервере SecurOS FaceX>. К именам камер, которые уже привязаны к направлениям прохода, добавляется в конце строчка «(используется)». Также существует возможность привязать используемую камеру к другому направлению прохода. В таком случае пользователь получит сообщение с подтверждением о новой привязке.

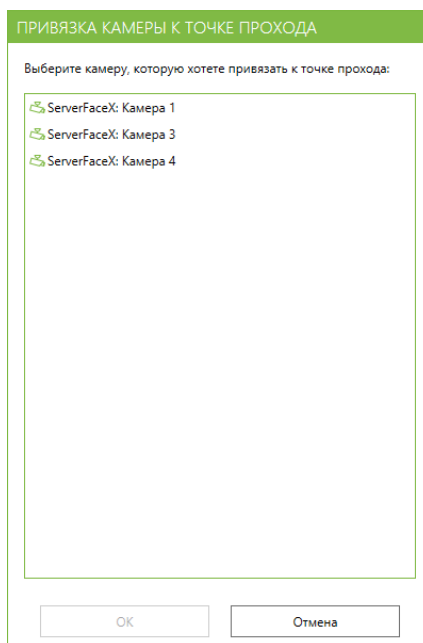


Рис. 13. Привязка камеры к направлению прохода

4.2.4 Настройка СКУД для двухфакторной аутентификации

Для обеспечения работы считывателя совместно с СБИ в режиме двухфакторной аутентификации необходимо, чтобы в настройках драйвера «Бастион-2 – ELSYS» для соответствующего считывателя была включена опция «Подтверждать доступ для карт с полномочиями "Доступ с подтверждением"» в блоке настроек «Полномочия дежурного оператора» (Рис. 14).

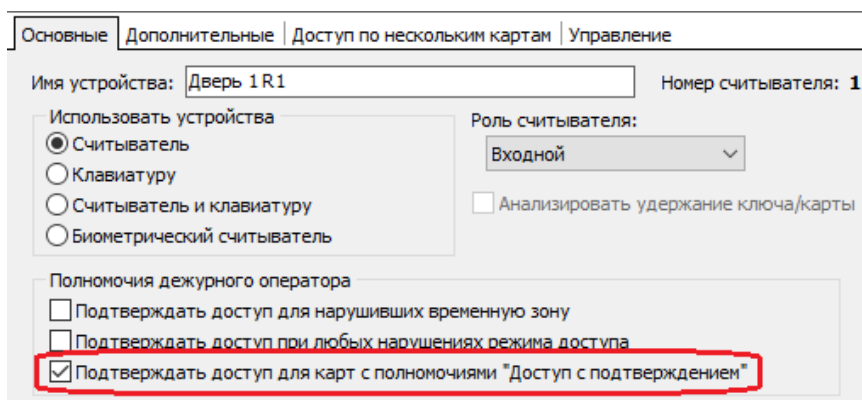


Рис. 14. Параметры точки прохода в настройках драйвера «Бастион-2 – ELSYS»

На вкладке «Дополнительные» необходимо включить опцию «Мониторинг предоставления доступа» (Рис. 15).

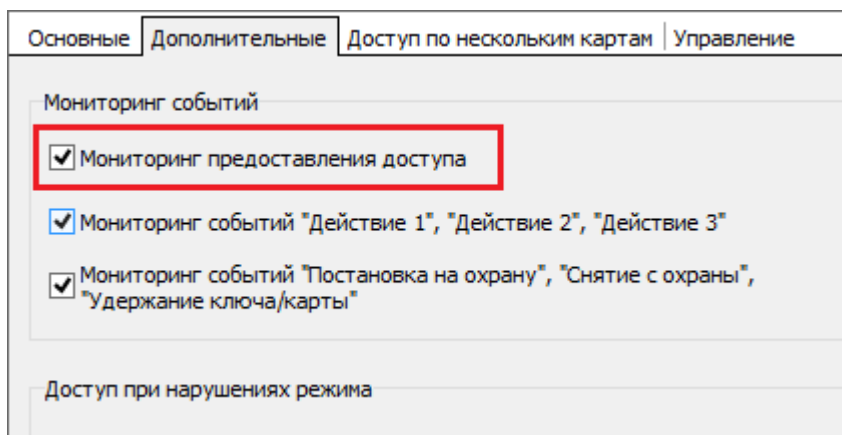


Рис. 15. Настройка мониторинга событий драйвера «Бастион-2 – ELSYS»

Для получения полной информации о настройке СКУД ELSYS следует ознакомиться с документом «Бастион-2 – ELSYS. Руководство администратора».

Всем пропускам, которые должны иметь доступ на считывателях, работающих в режиме двухфакторной аутентификации, должен быть задан уровень полномочий «Доступ с подтверждением» (Рис. 16).

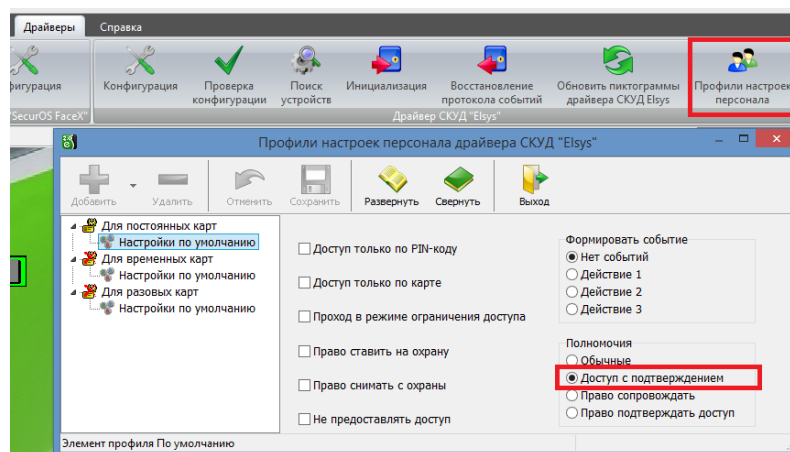


Рис. 16. Полномочия пропусков для доступа в режиме двухфакторной аутентификации

В случае применения последовательности прохода «сначала лицо потом карта» для режима двухфакторной аутентификации, использующий временный буфер распознанных лиц сервера SecurOS FaceX, необходимо провести дополнительные настройки:

- в основных настройках выбрать пункт «Использовать многофакторную СКУД-аутентификацию на сервере SecurOS FaceX» (см. пункт 4.2.2);
- в настройках сервера SecurOS FaceX выбрать только пункт «Многофакторная СКУД-аутентификация», настроить пункт «Время ожидания верификации» в диапазоне от 3000мс до 5000мс, указать в настройке «порог подобия для режима СКУД» 60 (см. Рис. 17).

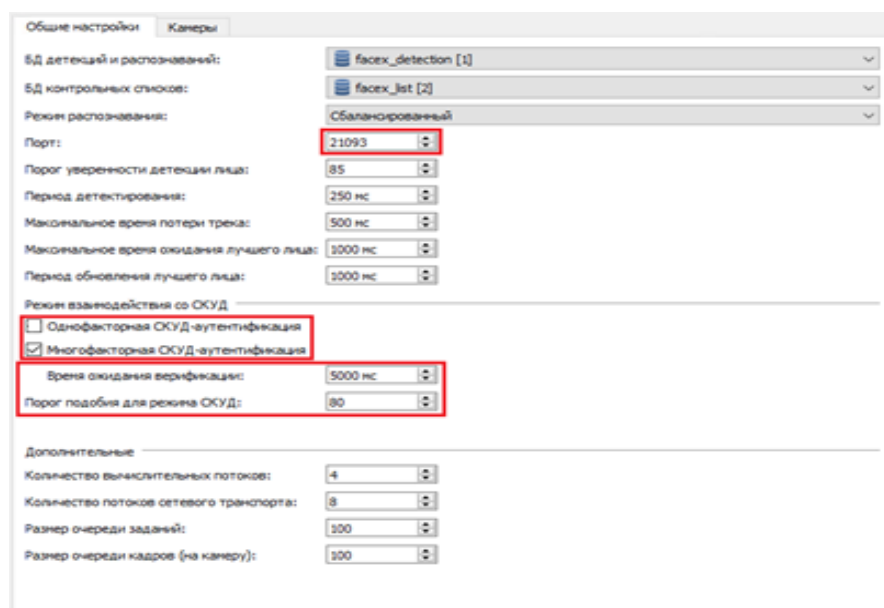


Рис. 17. Многофакторная СКУД-аутентификация

4.2.5 Виртуальные точки прохода

Виртуальная точка прохода не связана с реальным преграждающим устройством, но позволяет отслеживать местоположение персонала и посетителей в зонах, контролируемых камерами видеофиксации, подключенных 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).

Для создания новой виртуальной точки следует при выделенном в дереве узле «Виртуальные точки прохода» нажать кнопку «Добавить», для удаления существующей – кнопку «Удалить» при выделенной в дереве точке прохода, которую следует удалить. При сохранении настроек есть возможность удалить точки прохода без привязанной камеры.

Настройки виртуальной точки прохода представлены двумя параметрами, представленными на Рис. 18.

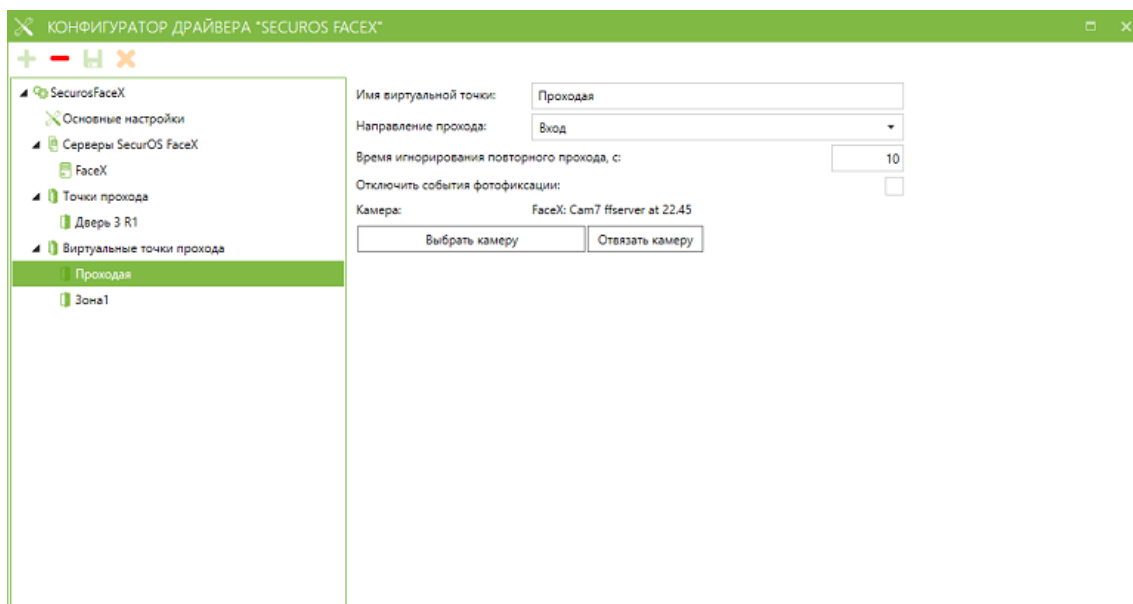


Рис. 18. Параметры виртуальной точки прохода

Имя виртуальной точки – текстовое название, присвоенное виртуальной точке прохода.

Камера – привязанная к виртуальной точке прохода камера. Процесс привязки камеры к виртуальной точке полностью аналогичен процессу привязки камеры к точке прохода ELSYS (пп. 4.3.3).

Направление прохода – вход\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;

Время игнорирования повторного прохода – время, в течение которого игнорируется повторный проход посетителя (по умолчанию 0 с).

Отключить события фотофиксации – при включении этой опции точка прохода не будет генерировать события «Зафиксировано лицо».

5 Работа в штатном режиме

5.1 Операции с пропусками

Все выдаваемые в АРМ «Бюро пропусков» пропуска с **фотографией** синхронизируются с серверами SecurOS FaceX в момент установки связи с ними.

При запуске драйвера происходит фоновая автоматическая синхронизация баз данных «Бастион - 2» и SecurOS FaceX. Процесс при первом запуске драйвера (когда база SecurOS пуста) может занимать от нескольких минут до нескольких часов (если БД содержит более 10000 пропусков). При последующих перезагрузках драйвер осуществляет быструю проверку баз данных, и обрабатывает все изменения, произошедшие за время его простоя. В период синхронизации идентификация будет осуществляться только по карточкам, уже попавшим в БД SecurOS FaceX.

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, также будет сгенерировано событие **«<ФИО посетителя>: не удалось синхронизировать пропуск с сервером SecurOS FaceX: <текст ошибки>»**.

5.2 Режим двухфакторной аутентификации

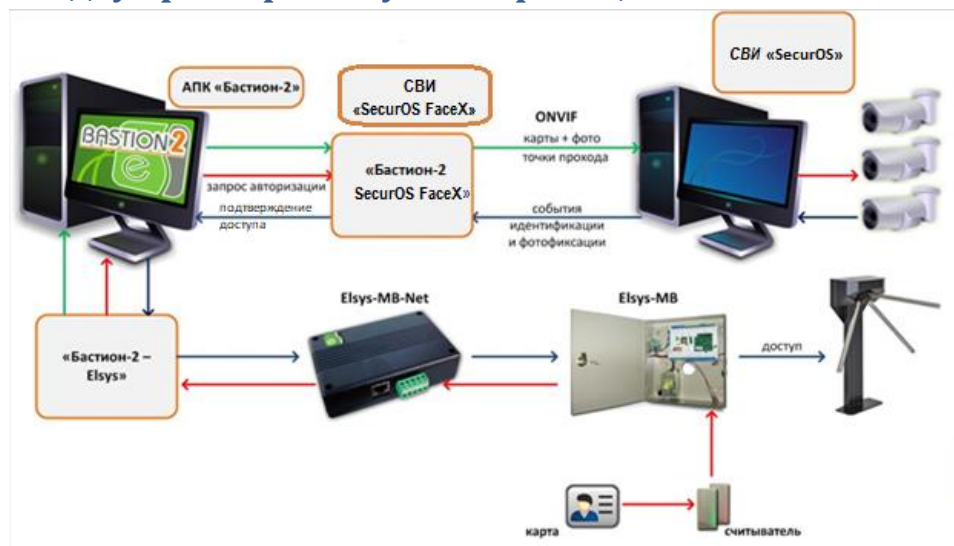


Рис. 19. Работа системы в режиме двухфакторной аутентификации

В режиме двухфакторной аутентификации посетитель сначала 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-2 – SecurOS FaceX». Далее модуль ожидает от сервера SecurOS FaceX событие об идентификации, и, если идентифицированный посетитель соответствует владельцу приложенной к считывателю карты, результат аутентификации передается обратно через драйвер «Бастион-2 – SecurOS FaceX» и драйвер «Бастион-2 – ELSYS» в контроллер (Рис. 19).

При появлении в поле зрения камеры лица, в APK «Бастион-2» будет сгенерировано событие **«<название точки прохода>: зафиксировано лицо»**, если генерация событий фотофиксации не отключена в настройках точки прохода.

Если личность посетителя была подтверждена по его изображению, то доступ будет предоставлен. В APK «Бастион-2» будет сгенерировано событие **«<название точки прохода>: доступ подтвержден <ФИО посетителя>»**.

Если в течение заданного времени ожидания сервером SecurOS FaceX не будет зафиксировано лица владельца приложенной карты, то в APK «Бастион-2» будет сгенерировано тревожное событие **«<название точки прохода>: в доступе отказано <ФИО посетителя>»**.

Если сервер SecurOS FaceX распознает возможную подмену лица владельца приложенной карты, то в APK «Бастион-2» будет сгенерировано тревожное событие **«<название точки прохода>: в доступе отказано <ФИО посетителя> возможна подмена»**.

К событиям «зафиксировано лицо» и «доступ подтвержден» прикрепляется фотография посетителя, полученная с камеры видеонаблюдения. Если соответствующая настройка включена в параметрах «Бастион-2», то фотография будет отображена в окне расширенного сообщения.

Внимание! Режим двухфакторной аутентификации требует наличия связи и работоспособности не только контроллеров ELSYS, но и модулей АПК «Бастион-2» 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 «Автоматически подтверждать доступ (Временная неисправность)».

5.3 Режим идентификации

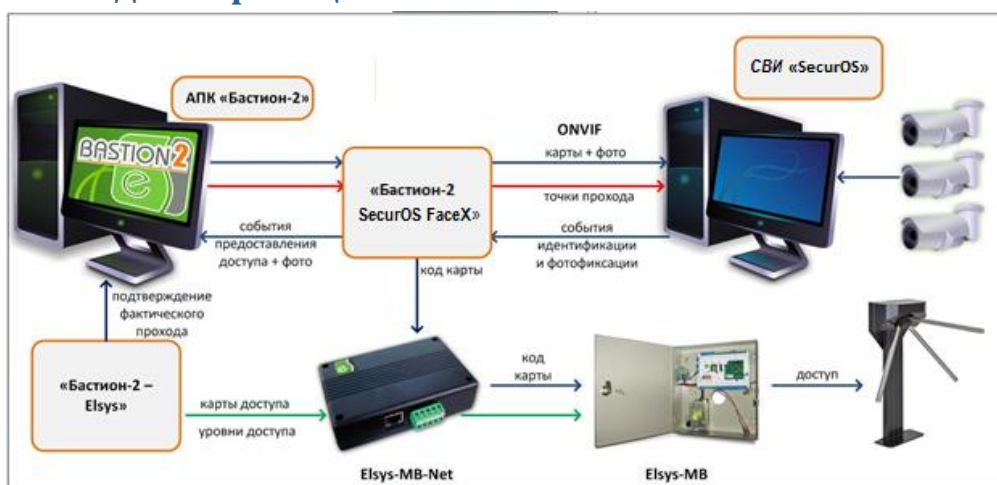


Рис. 20. Работа системы в режиме идентификации

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. СВИ SecurOS FaceX проанализирует изображение лица посетителя, полученное с камеры, и сравнит его с фотографиями всех активных пропусков, существующих в системе (Рис. 20).

При появлении в поле зрения камеры лица в «Бастион-2» будет сгенерировано событие «<название точки прохода>: зафиксировано лицо» с привязанной фотографией посетителя, полученной с камеры видеонаблюдения, если генерация событий фотофиксации не отключена в настройках направления прохода (п. 4.2.3).

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-2» будет сгенерировано событие (с привязанным изображением лица посетителя, полученным с камеры видеонаблюдения) «<название точки прохода>: предоставление доступа в режиме идентификации <ФИО посетителя>». При этом окончательное решение о допуске принимает СКУД ELSYS на основе имеющихся прав и уровней доступа.

Во всех случаях фотография, прикрепленная к генерируемому событию, будет отображена в окне расширенного сообщения (если включена соответствующая настройка в параметрах «Бастион-2»).

Внимание! При активации в основных настройках драйвера опции «Запрет обратного прохода в течение 7 секунд» доступ не будет предоставляться, если посетитель попытается выйти (с идентификацией по лицу) на точке прохода в обратном направлении в течение 7 секунд после прохода. В «Бастион-2» будет сгенерировано тревожное событие «<название точки прохода>: в доступе отказано <ФИО посетителя> (попытка обратного прохода в течение 7 секунд)».

5.4 Отслеживание прохода на виртуальных точках доступа

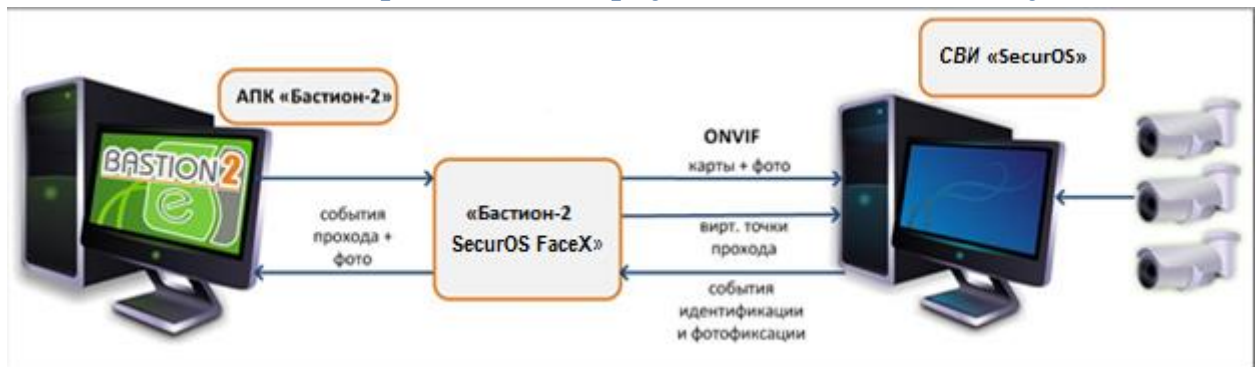


Рис. 21. Работа системы с виртуальными точками прохода

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. 21).

Если SecurOS FaceX обнаружит в системе активный пропуск, имеющий фотографию лица, совпадающего с лицом на изображении, полученного с камеры видеонаблюдения, то в АПК «Бастион-2» будет сгенерировано событие **«Вход в зону <ФИО посетителя>»** или **«Выход из зоны <ФИО посетителя>»**.

Если SecurOS FaceX обнаружит подмену лица для активного пропуска в системе, то в АПК «Бастион-2» будет сгенерировано событие **«Вход в зону <ФИО посетителя> возможна подмена»** или **«Выход из зоны <ФИО посетителя> возможна подмена»**.

Если соответствующая настройка включена в параметрах АПК «Бастион-2», то фотография, прикрепляемая к событиям, будет отображена в окне расширенного сообщения.

6 Нештатные ситуации

В случае потери связи с сервером «SecurOS FaceX» в «Бастион-2» будет сгенерировано событие **«Потеряно соединение с сервером SecurOS FaceX»**. При восстановлении связи будет сгенерировано событие **«Установлено соединение с сервером SecurOS FaceX»**.

Режим двухфакторной аутентификации требует наличия связи и работоспособности не только контроллеров ELSYS, но и модулей АПК «Бастион-2» 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 устанавливать опцию «Автоматически подтверждать доступ (Временная неисправность)». Также, рекомендуется всегда включать опцию «Автоматически подтверждать доступ при потере связи с серверами SecurOS FaceX при двухфакторной аутентификации».



Приложения

Приложение 1. История изменений

1.0.4 (14.07.2022)

[+] Поддержка серверов SecurOS версии 11.1

1.0.3 (04.10.2021)

[+] Поддержка серверов SecurOS версии 10.9.

[+] Добавлена поддержка для работы с драйвером «Бастиян-2-Elsys 2.0».

[+] Добавлено получения сведений о наличии маски на лице человека во всех режимах работы драйвера.

[+] Виртуальные точки прохода теперь представлены в системе и дверью, и считывателем. Таким образом, их можно использовать и в уровнях доступа, и в областях контроля.

[+] Добавлена возможность настройки интервала времени для подтверждения прохода распознанной персоны.

[+] Поддержка серверов SecurOS версии 10.7.

[*] Исправлена работа двухфакторной аутентификации, использующий режим многофакторной СКУД-аутентификации сервера SecurOS FaceX (сначала лицо, потом карта).

[*] Исправления в терминологии и документации.

1.0.2 (01.09.2020)

[+] Поддержка серверов SecurOS версии 10.6.

1.0.1 (20.03.2020)

[+] Первая версия, включена в комплект поставки АПК «Бастиян-2».