Бастион-3 – Face. Руководство администратора

Версия 2024.3

(25.10.2024)

Самара, 2024

Оглавление

1 Общие сведения

1.1 Назначение и область применения

Драйвер «Бастион-3 – Face» предназначен для подключения к ПК «Бастион-3» внешних систем сторонних производителей. Взаимодействие со внешними системами производится с использованием протокола на основе стандарта ONVIF Profile A, C.

Интеграция может быть выполнена силами производителей внешней системы. Для получения подробной информации о возможностях и способах интеграции, следует обратиться с соответствующим запросом в отдел технической поддержки ГК «ТвинПро».

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 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 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 ко внешней системе.

2 Условия применения

2.1 Требования к совместимости

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

Для работы модуля с настройками по умолчанию на сервере оборудования должен быть открыт сетевой порт для входящих подключений (по умолчанию это порт 8089), который можно изменить в настройках.

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

Для обмена данными между модулем «Бастион-3 – Face» и внешней системой используется протокол ONVIF Profile A, C.

Модуль совместим с ПК «Бастион-3» версии 2023.1 и выше.

2.2 Лицензирование системы

Для работы модуля требуется дополнительная лицензия.

Лицензирование производится по числу обслуживаемых системой *направлений прохода*. Исп. 1 предназначено для биометрической идентификации 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 – Face Исп. 1». Число необходимых лицензий не зависит от числа видеокамер, используемых для каждого направления прохода.

Стоимость лицензий на «Бастион-3 – Face» не включает стоимость внешних систем.

3 Установка системы

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

В ОС Windows установка производится путем запуска файла инсталлятора FaceSetup.msi.

В ОС Linux необходимо установить пакет bastion3-driver-face_*.deb или bastion3-driver-face_*.rpm.

4 Настройка системы

4.1 Добавление драйвера «Бастион-3 – Face»

Для запуска драйвера следует добавить его экземпляр в конфигурацию ПК «Бастион-3» через панель управления. Добавление драйверов ПК «Бастион-3» описано в документе «*Бастион-3. Руководство администратора*».

4.2 Настройка драйвера

Настройка драйвера осуществляется при помощи специального конфигуратора. Для его запуска следует нажать на кнопку «Конфигурация», располагающуюся в блоке драйвера «Бастион-3 – Face» на вкладке «Драйверы».

Окно конфигуратора представлено на Рис. 1 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 внешних систем.
3. Добавить направления прохода и определить режимы доступа для них.
4. Добавить необходимые виртуальные точки прохода и задать их направления.
5. Настроить соответствия точек прохода и видеокамер (выполняется на стороне внешней системы).
6. Настроить СКУД для двухфакторной аутентификации, если этот режим доступа используется.

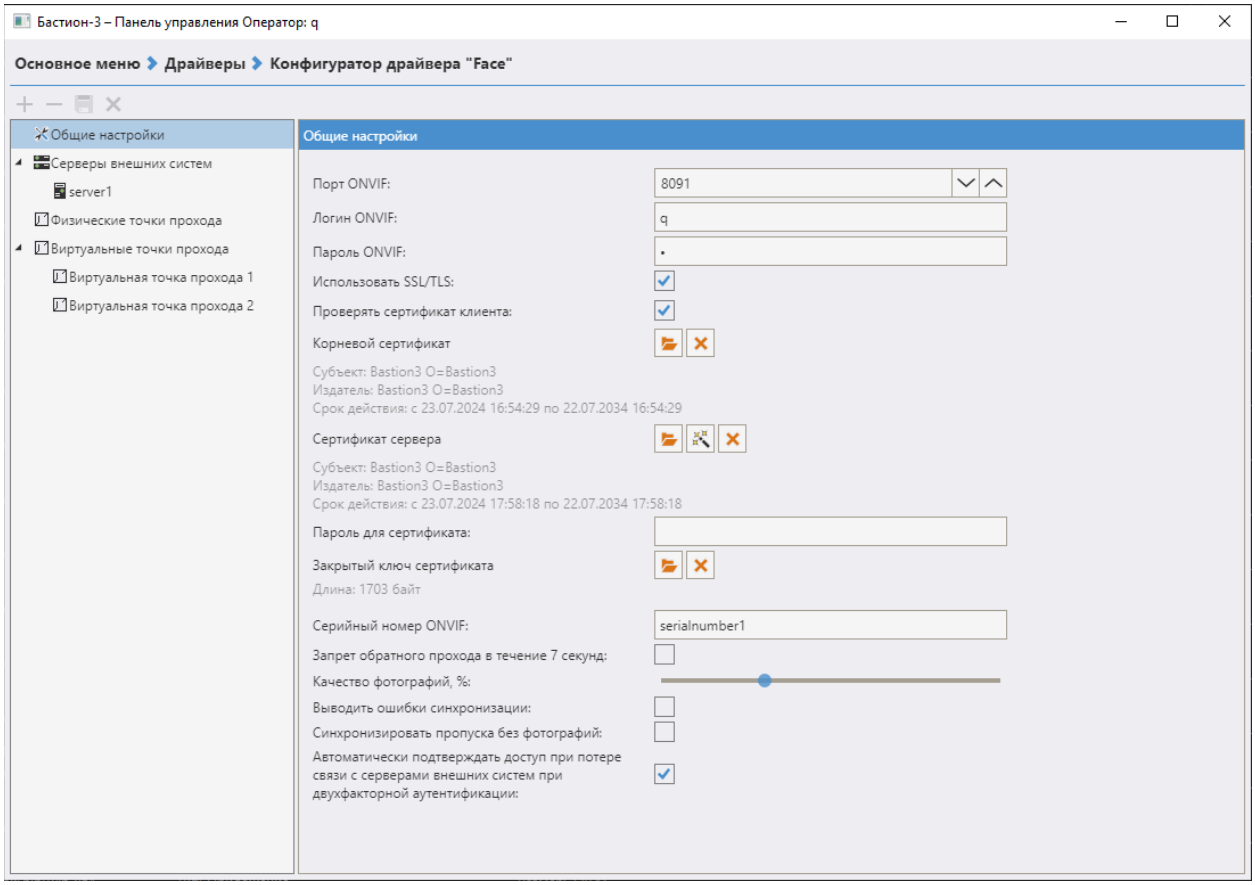

Рис. 1. Конфигуратор драйвера «Бастион-3 – Face»

4.2.1 Основные настройки

В основных настройках определяются следующие параметры:

Автоматически подтверждать доступ при потере связи со внешними системами при двухфакторной аутентификации (включено по умолчанию) – при включенной настройке, в случае потери связи драйвера «Бастион-3 – Face» со внешними системами, драйвер будет

выдавать автоматическое подтверждение доступа для всех карт, по которым такое подтверждение будет запрошено. Если настройка отключена, то при отсутствии связи со внешними системами доступ в режиме двухфакторной аутентификации предоставляться не будет.

Порт ONVIF – сетевой порт, на котором будут выполняться ONVIF-службы модуля. Значение должно быть числом в диапазоне 1 – 65535. Для обеспечения связи ПК «Бастион-3» с сервером внешней системы данный порт должен быть свободен и открыт в сетевых экранах (по умолчанию – 8089).

Логин ONVIF/пароль ONVIF – логин и пароль для Digest-аутентификации. Пара логин/пароль используется для защиты данных, передаваемых с сервера внешней системы.

Использовать SSL/TLS – при установке флага будет использоваться защищённое соединение с клиентской частью внешней системы. При этом возможна взаимная проверка сертификатов сервера и клиента при установке соединения.

Проверять сертификат клиента — если флаг установлен, при подключении клиента сервер будет проверять действительность его сертификата.

Корневой сертификат — если указан, то валидность сертификата клиента будет проверяться этим сертификатом. Здесь может быть указан файл с публичной частью сертификата клиента, либо файл с публичной частью корневого сертификата клиента.

Сертификат сервера — сертификат, который будет использоваться сервером при установке соединения. Самоподписанный сертификат сервера можно сгенерировать, нажав кнопку «  ».

Пароль для сертификата — здесь необходимо ввести пароль сертификата сервера, если сертификат защищён паролем.

Закрытый ключ сертификата — здесь необходимо загрузить приватный ключ сертификата, если он хранится отдельно от публичной части сертификата в формате PEM.

Серийный номер ONVIF – это поле нужно заполнить серийным номером ПК «Бастион-3».

Запрет обратного прохода в течение 7 секунд – при включении этой опции доступ не будет предоставляться, если посетитель попытается выйти (с идентификацией по лицу) на точке прохода в обратном направлении в течение 7 секунд после прохода.

Качество фотографий, % – качество сжатия изображений с видеокамер, передаваемых из внешней системы в ПК «Бастион-3» при событиях прохода. Следует иметь ввиду, что эти фотографии используются для:

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

Не рекомендуется выставлять положение ползунка близко к максимальному значению шкалы, так как это сильно увеличивает занимаемое сохраняемыми в базе данных изображениями дисковое пространство.

Синхронизировать пропуска без фотографий – при отключении этой настройки пропуска без фотографии не будут загружаться на сервера внешних систем.

4.2.2 Настройка соединений с серверами внешних систем

Узел дерева настроек «Серверы внешних систем» группирует настроенные подключения к серверам внешних систем (ис. 2). Для добавления нового сервера следует нажать кнопку «Добавить» на панели инструментов конфигуратора, для удаления – кнопку «Удалить». Настройки подключения к серверу внешней системы представлены следующими параметрами:

- Название сервера;
- Адрес службы управления профилям персон;
- Логин для подключения к службе управления профилями персон;
- Пароль для подключения к службе управления профилями персон;
- Адрес службы событий;
- Логин для подключения к службе событий;
- Пароль для подключения к службе событий;
- Использовать SSL/TLS;
- Проверять сертификат сервера;
- Проверять имя сервера;
- Корневой сертификат;
- Отправлять сертификат клиента;
- Сертификат клиента;
- Пароль для сертификата;
- Закрытый ключ сертификата.

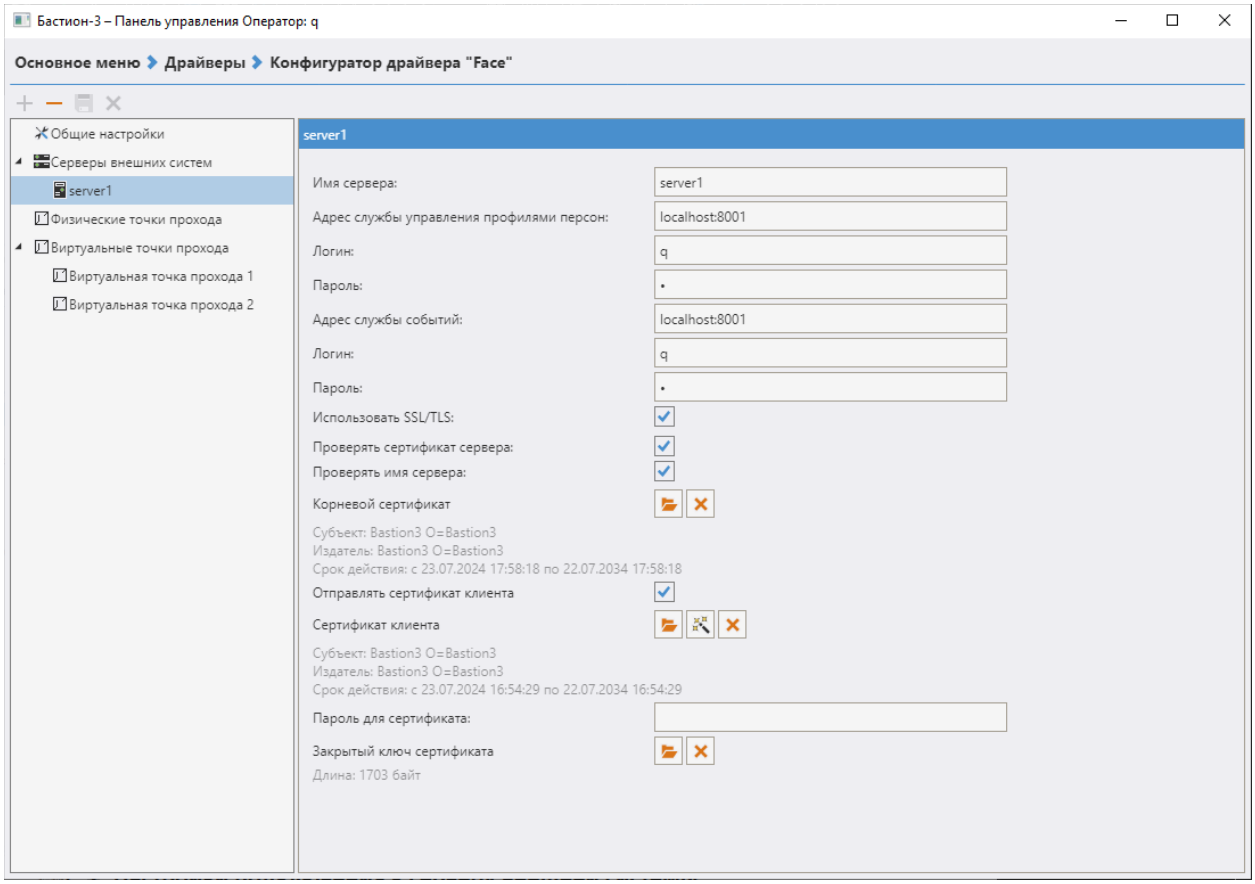

Рис. 2. Настройки подключения к серверу внешней системы

4.2.3 Физические точки прохода

Узел конфигурации «Физические точки прохода» содержит направления прохода СКУД (считыватели), подключенные ко внешней системе. Для подключения считывателей следует выделить узел настроек «Физические точки прохода» и нажать кнопку «Добавить» на панели инструментов, в результате чего откроется окно добавления считывателей (Рис. 3). Для отключения направления прохода от внешних систем необходимо выделить направление прохода в дереве конфигурации и нажать кнопку «Удалить».

В рамках драйвера «Бастион-3 – Face» каждому направлению прохода соответствует считыватель СКУД ELSYS. Настройка соответствия точек прохода и видеокамер внешних систем должно производиться в модуле конфигурации самой внешней системы.

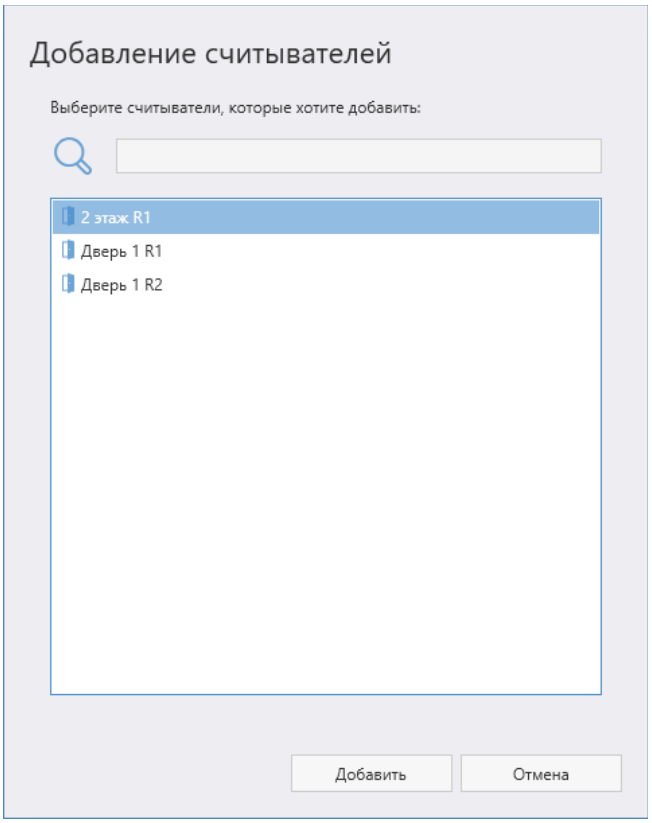

Рис. 3: Добавление считывателей

Настройки подключенного направления прохода (Рис. 4) представлены двумя параметрами, которые описаны ниже.

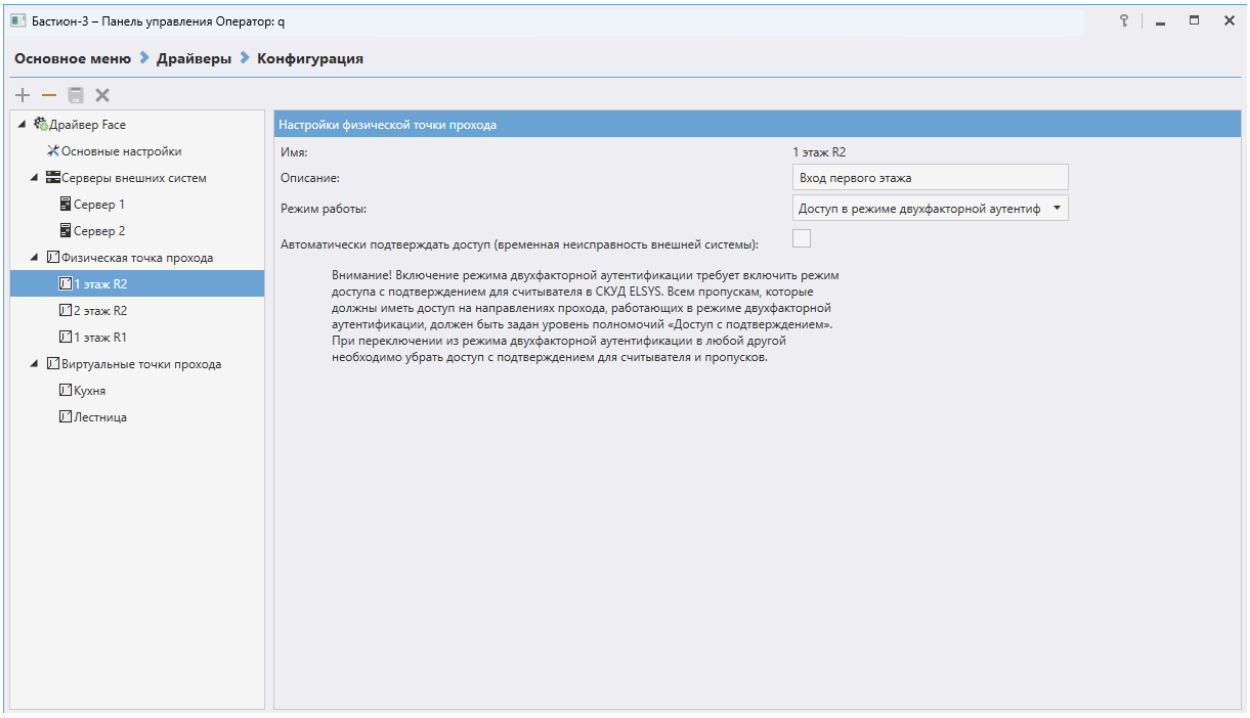

Рис. 4. Параметры направления прохода

Описание – текстовое описание, комментарий к направлению прохода. Передаётся на серверы внешних систем. Описание служит для облегчения идентификации направления прохода при настройке связей камер видеонаблюдения с направлениями прохода СКУД при конфигурировании внешних систем. Значение настройки может содержать примерное описание местоположения направления прохода.

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

- *Доступ только по карте* – в этом режиме направление 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 посетитель сначала прикладывает карту к считывателю, затем сервер внешней системы сопоставляет изображение, полученное с привязанной камеры, с фотографией посетителя, которая сохранена в «Бастион-3», и выдает подтверждение / отказ в доступе.

Автоматически подтверждать доступ (временная неисправность внешней системы) – опцию следует включать в режиме двухфакторной аутентификации только в том случае, если необходимо временно отключить подтверждение доступа через внешнюю систему, то есть – в случае временной неисправности внешней системы. Если опция включена, драйвер «Бастион-3 – Face» будет самостоятельно давать подтверждение всем картам, по которым оно будет запрашиваться, не отправляя запрос во внешнюю систему. Настройка позволяет не отключать доступ с подтверждением для пропусков и считывателей, отключив временно фактический запрос подтверждения через внешнюю систему.

4.2.4 Настройка СКУД для двухфакторной аутентификации

Для обеспечения работы направления прохода совместно со внешней системой в режиме двухфакторной аутентификации необходимо, чтобы в настройках драйвера «Бастион-3 – ELSYS» для соответствующего считывателя была включена опция «Подтверждать доступ для карт с полномочиями "Доступ с подтверждением"» в блоке настроек «Полномочия дежурного оператора» (Рис. 5). Для получения информации о настройке СКУД ELSYS следует ознакомиться с документом «Бастион-3 – ELSYS. Руководство администратора».

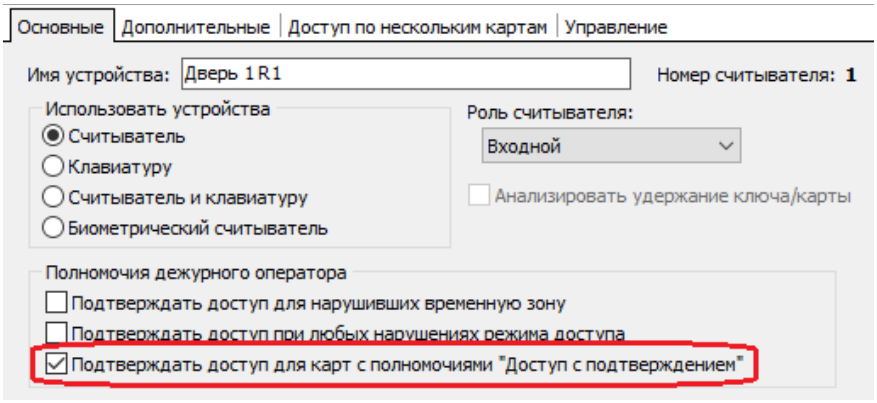

Рис. 5. Параметры считывателя в настройках драйвера «Бастион-3 – ELSYS»

Всем пропускам, которые должны иметь доступ на направлениях прохода, работающих в режиме двухфакторной аутентификации, должен быть задан уровень полномочий «Доступ с подтверждением» (Рис. 6).

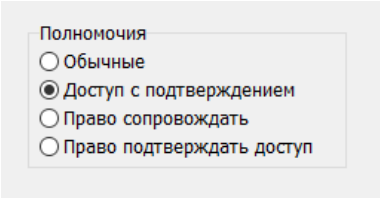

Рис. 6. Полномочия пропусков для доступа в режиме двухфакторной аутентификации

Внимание! *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). Направления прохода контроллеров ELSYS MB-IP можно подключать ко внешним системам только в режиме двухфакторной аутентификации.*

4.2.5 Виртуальные точки прохода

Этот узел дерева настроек группирует 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 ко внешней системе.

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.

Настройки виртуальной точки прохода представлены тремя параметрами (Рис. 7).

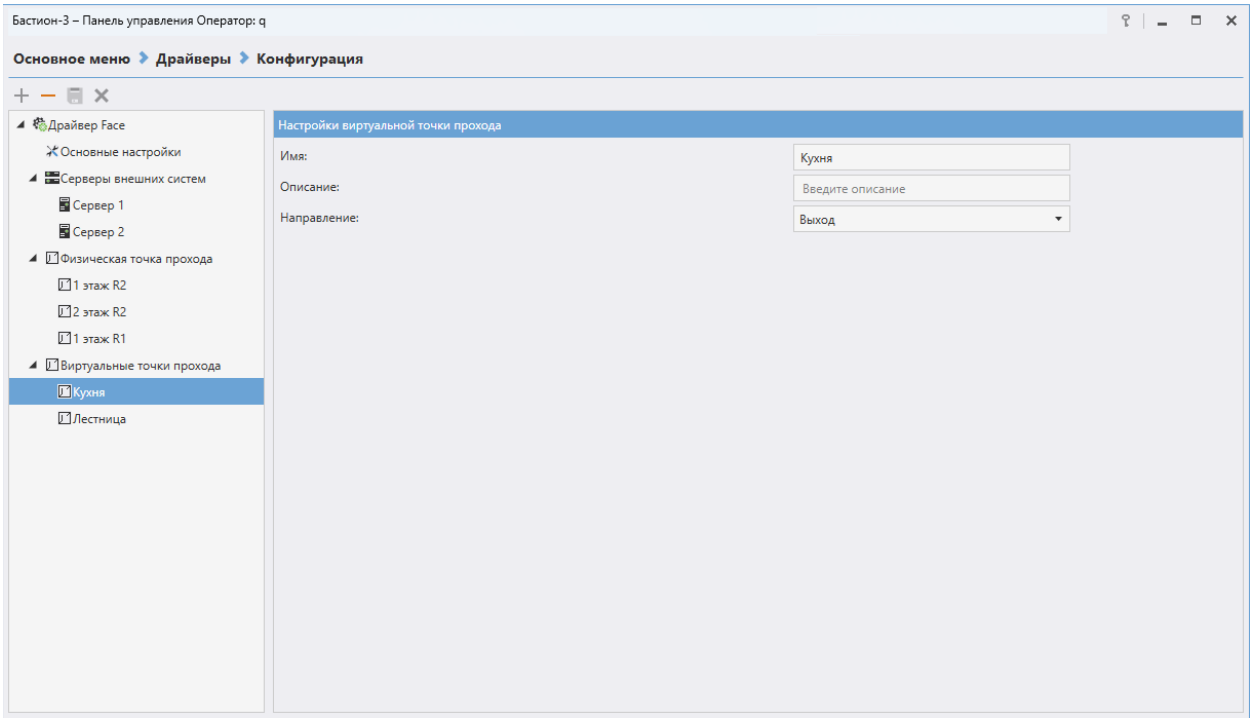

Рис. 7. Параметры виртуальной точки прохода

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

Описание – текстовое описание с примерным местоположением камеры, к которой будет привязана виртуальная точка прохода.

Направление – вход или выход, от этой настройки будут зависеть генерируемые точкой события.

5 Работа в штатном режиме

5.1 Синхронизация списка пропусков

Все выдаваемые пропуска **с фотографией** синхронизируются с серверами внешних систем в момент подключения к серверам внешних систем.

> ***Внимание!*** *В некоторых системах биометрической идентификации у посетителя не может быть более одной активной (выданной) карты доступа. В этом случае, при попытке синхронизации с сервером внешней системы пропуска, имеющего фотографию, на которой изображен человек, уже имеющий другой активный пропуск, сервер вернёт ошибку. При этом в ПК «Бастион-3» будет сгенерировано событие об ошибке синхронизации пропуска.*

При обновлении фотографии или ФИО владельца пропуска изменения отправляются автоматически на сервера внешних систем.

В случае, если идентификация пользователя СКУД по фотографии из ПК «Бастион-3» происходит с низкой вероятностью, то следует произвести настройки на стороне внешней системы (снизить порог распознавания, добавить дополнительные фотографии). Подробно об этих операциях см. документацию ко внешней системе.

5.2 Режим двухфакторной аутентификации

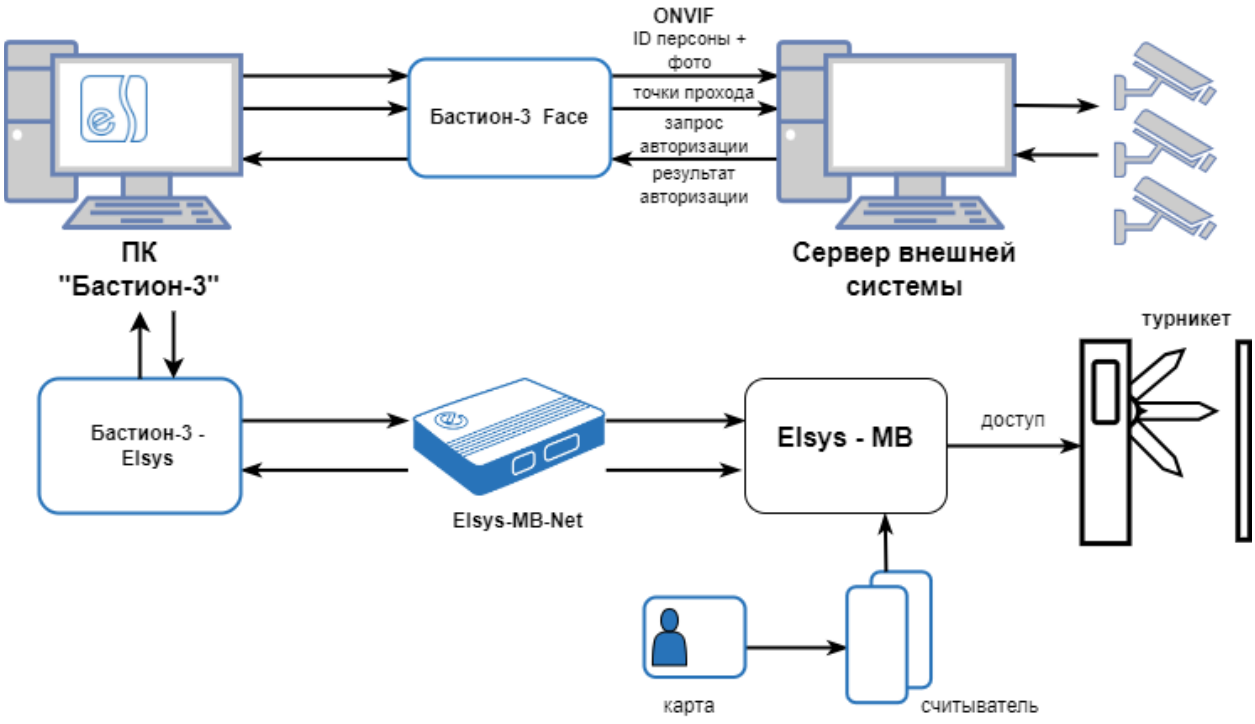

Рис. 8. Работа системы в режиме двухфакторной аутентификации

В режиме двухфакторной аутентификации посетитель сначала прикладывает пропуск к считывателю. При этом его лицо должно быть в зоне обзора камеры видеонаблюдения, которая контролирует направление прохода. Контроллер Elsys-MB проверяет права предъявленной карты доступа. Если для карты активна опция «Доступ с подтверждением», то контроллер выдает запрос внешней аутентификации карты, который передается во внешнюю систему модулем «Бастион-3 – Face». Внешняя система анализирует изображение лица посетителя, полученное с камеры, и принимает решение о соответствии лица с полученного изображения и лица с фотографии, сохранённой в данных пропуска. Результат аутентификации передается обратно от внешней системы, через драйвер «Бастион-3 – Face» и драйвер «Бастион-3 – ELSYS» в контроллер (Рис. 8).

Если лица не соответствуют (посетитель прикладывает карту доступа, выданную не ему), то доступ предоставлен не будет. В «Бастион-3» будет сгенерировано тревожное событие **«*<название направления прохода>*: в доступе отказано *<ФИО посетителя>*»**.

Если личность посетителя была подтверждена по его изображению, то доступ будет предоставлен. В «Бастион-3» будет сгенерировано событие **«*<название направления прохода>*: доступ подтвержден *<ФИО посетителя>*»**.

В обоих случаях к генерируемому событию будет прикреплено изображение посетителя, полученное с камеры видеонаблюдения (если лицо посетителя попало в область обзора камеры). 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 внешней системы. В случае неисправности хотя бы одного из компонентов, подтверждение доступа для карт передаваться не будет и в доступе будет отказано. В случае неисправности внешней системы рекомендуется для соответствующих точек прохода временно устанавливать опцию «Автоматически подтверждать доступ (Временная неисправность внешней системы)». Также, рекомендуется всегда включать опцию «Автоматически подтверждать доступ при потере связи с серверами внешних систем при двухфакторной аутентификации».*

5.3 Режим идентификации

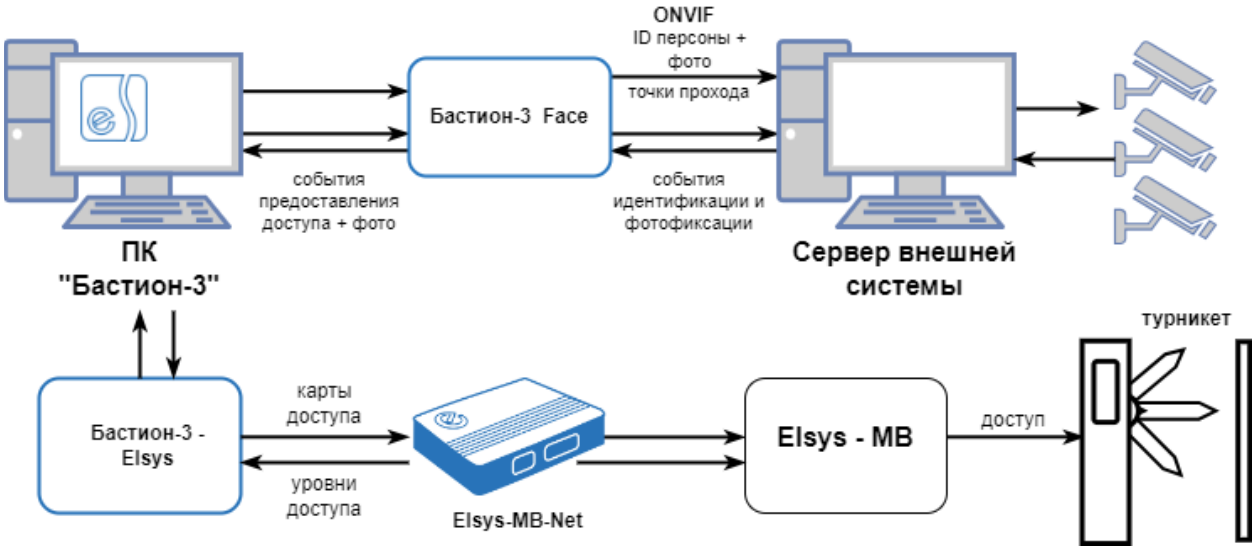

Рис. 9. Работа системы в режиме идентификации

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 направлении прохода посетителю достаточно встать напротив камеры видеонаблюдения. Внешняя система проанализирует изображение лица посетителя, полученное с камеры, и сравнит его с фотографиями всех активных пропусков, существующих в системе (Рис. 9).

Если внешняя система 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 сгенерировано событие (с привязанным изображением лица посетителя, полученным с камеры видеонаблюдения) «***<название направления прохода>:*** **доступ в режиме идентификации** ***<ФИО посетителя>***». При этом окончательное решение о допуске принимает СКУД ELSYS на основе имеющихся прав и уровней доступа.

В случае, если посетитель не будет идентифицирован по лицу (не найден активный пропуск с фотографией, на которой изображено лицо, совпадающее с изображения с камеры), доступ не

будет предоставлен, а в «Бастион-3» будет сгенерировано тревожное событие ***«<название направления прохода>: в* доступе отказано»**, к которому будет привязано изображение, полученной с камеры видеонаблюдения.

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

> ***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-3» будет сгенерировано тревожное событие* ***«<название направления прохода>: в доступе отказано <ФИО посетителя> (попытка обратного прохода в течение 7 секунд)».***

5.4 Отслеживание прохода на виртуальных точках доступа

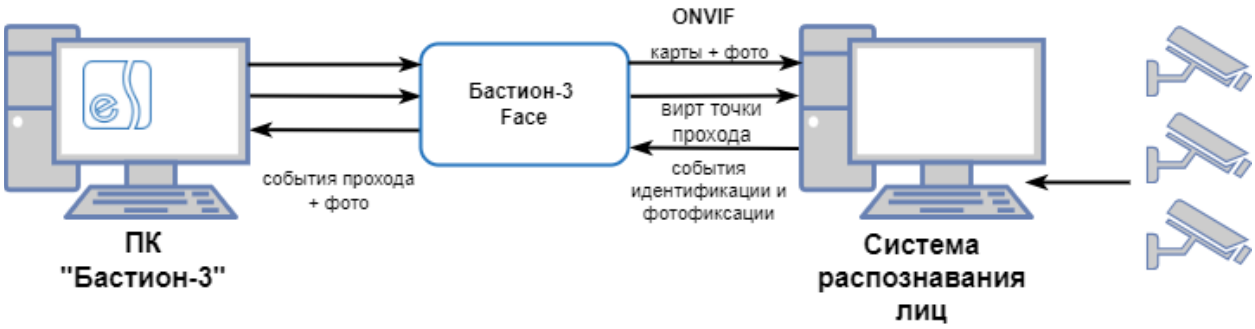

Рис. 10. Работа системы с виртуальными точками прохода

Для виртуальной точки прохода внешняя система будет генерировать события при обнаружении лица в области видимости камеры наблюдения (Рис. 10).

Если внешняя система обнаружит в системе активный пропуск, имеющий фотографию лица, совпадающего с лицом на изображении, полученного с камеры видеонаблюдения, то в «Бастион-3» будет сгенерировано событие **«Штатный вход *<ФИО посетителя>*»** или **«Штатный выход *<ФИО посетителя>*»** в зависимости от направления виртуальной точки прохода.

В случае, если посетитель не будет идентифицирован по лицу с изображения, полученного с камеры (не найден активный пропуск с фотографией, на которой изображено лицо, совпадающее с изображения с камеры), в «Бастион-3» будет сгенерировано тревожное событие **«Вход неизвестного лица»** или **«Выход неизвестного лица»** в зависимости от направления виртуальной точки прохода.

В обоих случаях к генерируемому событию будет прикреплено изображение посетителя, полученное с камеры видеонаблюдения. Если соответствующая настройка включена в параметрах «Бастион-3», то фотография будет отображена в окне расширенного сообщения.

5.5 Дополнительная информация в событиях

В зависимости от возможностей используемой внешней системы, ко всем основным событиям идентификации, фотофиксации и запрета доступа может прикрепляться дополнительная информация о наличии/отсутствии лицевой маски на фотографии человека, а также о повышенной температуре тела. Пример такого события:

«*<название направления прохода>:* доступ в режиме идентификации *<ФИО посетителя>. Повышена температура (37.8), отсутствует маска*».

Предполагается, что решение о предоставлении доступа на основе признаков наличия маски и повышенной температуры принимает внешняя система.

6 Нештатные ситуации

В случае потери связи с сервером внешней системы в «Бастион-3» будет сгенерировано событие **«Потеряно соединение с сервером внешней системы»**. При восстановлении связи будет сгенерировано событие **«Установлено соединение с сервером внешней системы»**.

Режим двухфакторной аутентификации требует наличия связи и работоспособности не только контроллеров ELSYS, но и модулей ПК «Бастион-3» и внешней системы. В случае неисправности хотя бы одного из компонентов, подтверждение доступа для карт передаваться не будет и в доступе будет отказано. В случае неисправности внешней системы рекомендуется для соответствующих точек прохода временно устанавливать опцию «Автоматически подтверждать доступ (Временная неисправность внешней системы)». Также, рекомендуется всегда включать опцию «Автоматически подтверждать доступ при потере связи с серверами внешних систем при двухфакторной аутентификации».

В процессе синхронизации пропусков с сервером внешней системы возможны ситуации, когда фотография на пропуске не будет удовлетворять предъявляемые системой распознавания лиц требования к качеству изображения (например, система не сможет найти на картинке лицо человека). В таком случае будет сгенерировано событие **«<ФИО посетителя>: не удалось синхронизировать пропуск с сервером внешней системы: <текст ошибки>»**.

Приложения

Приложение 1. Список событий

Таблица 1. Список событий

Устройство	Событие	Условия возникновения
Система	Превышено лиц. ограничение (получено %s2 из %s1)	Возникает, если в ключе защиты записано исполнение меньше, чем реально используется.
Дверь	Штатный вход %s1	Для виртуальных точек прохода возникает при обнаружении известного лица в зоне обзора соответствующей камеры, если направление

		виртуальной точки - вход
Дверь	Штатный выход %s1	Для виртуальных точек прохода возникает при обнаружении известного лица в зоне обзора соответствующей камеры, если направление виртуальной точки - выход
Дверь	Вход неизвестного лица	Для виртуальных точек прохода возникает при обнаружении неизвестного лица в зоне обзора соответствующей камеры, если направление виртуальной точки - вход
Дверь	Выход неизвестного лица	Для виртуальных точек прохода возникает при обнаружении неизвестного лица в зоне обзора соответствующей камеры, если направление виртуальной точки - выход
Сервер	Установлено соединение с сервером внешней системы	При успешной установке связи с сервером внешней системы
Сервер	Потеряно соединение с сервером внешней системы	При потере связи с сервером внешней системы
Сервер	%s1: не удалось синхронизировать пропуск с сервером внешней системы: %s2	При ошибке синхронизации данных пропуска с сервером внешней системы
Виртуальное устройство 1	Доступ подтверждён %s1. %s2	При успешном подтверждении доступа сервером внешней системы в режиме двухфакторной аутентификации
Виртуальное устройство 1	Доступ в режиме идентификации %s1. %s2	При предоставлении доступа сервером внешней системы в режиме идентификации
Виртуальное устройство 1	В доступе отказано %s1. %s2"	При отказе в доступе сервером внешней системы с указанием дополнительных признаков (маски, температуры)
Виртуальное устройство 1	В доступе отказано. %s2	При отказе в доступе сервером внешней системы
Виртуальное устройство 1	В доступе отказано %s1 (попытка обратного прохода в течение 7 секунд). %s2	При активации в основных настройках драйвера опции «Запрет обратного прохода в течение 7 секунд», если посетитель попытается выйти (с идентификацией по лицу) на точке прохода в обратном направлении в течение 7 секунд после прохода.
Виртуальное	В доступе отказано (попытка	При обнаружении сервером внешней системы

устройство 1	прохода по фото). %s2	попытки прохода по фотографии вместо реального лица.
Виртуальное устройство 1	В доступе отказано %s1 (попытка прохода по фото). %s2	При обнаружении сервером внешней системы попытки прохода по фотографии вместо реального лица с указанием дополнительных признаков.
Виртуальное устройство 1	Зафиксировано нарушение (%s2).	При обнаружении сервером внешней системы нарушений при проходе неизвестного лица (например, «проход над турникетом» или «повышенная температура»), с указанием типа нарушения.
Виртуальное устройство 1	Зафиксировано нарушение: %s1 (%s2).	При обнаружении сервером внешней системы нарушений при проходе известного лица (например, «проход над турникетом» или «повышенная температура»), с указанием типа нарушения.

Приложение 2. История изменений

2024.2

[+] Добавлена поддержка mTLS.

[*] Исправлено отображение состояния установки модуля в «Мониторе состояний».

1.0.1 (27.04.2023)

[+] Первая версия драйвера добавлена в комплект поставки ПК «Бастион-3».