Бастион-2 – Face. Руководство администратора

Версия 1.1.3

(25.05.2026)

Самара, 2026

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 Добавление драйвера «Бастион-2 – Face»....3
4.2 Настройка драйвера....3
4.2.1 Основные настройки....4
4.2.2 Настройка соединений с серверами внешних систем....5
4.2.3 Направления прохода....6
4.2.4 Настройка СКУД для двухфакторной аутентификации....8
4.2.5 Виртуальные точки прохода....9
5 Работа в штатном режиме....10
5.1 Синхронизация списка пропусков....10
5.2 Режим двухфакторной аутентификации....11
5.3 Режим идентификации....12
5.4 Отслеживание прохода на виртуальных точках доступа....13
5.5 Дополнительная информация в событиях....13
6 Нештатные ситуации....14
Приложения....14
Приложение 1. Список событий....14
Приложение 2. История изменений....16

1 Общие сведения

1.1 Назначение и область применения

Модуль «Бастион-2 – Face» предназначен для подключения к АПК «Бастион-2» комплексов биометрической идентификации (внешних систем) сторонних производителей, а также любых систем, которые могут использоваться для предоставления / подтверждения доступа. Взаимодействие с внешними системами производится с использованием протокола на основе стандарта ONVIF Profile A, C.

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

Модуль обеспечивает возможности передачи подтверждений доступа для СКУД ELSYS (ООО «ЕС-пром», ГК «ТвинПро») на основе проверок, выполняемых во внешней системе, а также возможность передачи номера карты доступа по интерфейсу управления сетевым контроллером Elsys MB-Net.

Таким образом, модуль позволяет использовать как режим двухфакторной аутентификации (например, 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.

Модуль также предоставляет опциональную возможность синхронизации списка пропусков АПК «Бастион-2» с внешней системой, включая фотографии.

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 внешними системами (например, камерами видеофиксации, подключенных к серверам внешних систем).

2 Условия применения

2.1 Требования к совместимости

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

Для работы модуля с настройками по умолчанию на сервере оборудования должен быть открыт сетевой порт 8089. Порт можно изменить в настройках.

Для работы с реальными точками прохода требуется наличие СКУД ELSYS и драйвера «Бастион-2 – ELSYS». Доступ в режиме идентификации (например, 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.

Модуль версии 1.1.2 совместим с АПК «Бастион-2» версии 2.1.12 и выше. Модули более ранних версий совместимы с АПК «Бастион-2» версии 2.1.1 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-2 – Face Исп. 1». Число необходимых лицензий не зависит от числа видеокамер, используемых для каждой точки прохода.

Стоимость лицензий на «Бастион-2 – Face» не включает стоимость любых модулей внешних систем.

3 Установка системы

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

4 Настройка системы

4.1 Добавление драйвера «Бастион-2 – Face»

Для запуска драйвера следует добавить его экземпляр в конфигурацию АПК «Бастион-2». Добавление драйверов АПК «Бастион-2» описано в документе «*Бастион-2. 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-2 – 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.
5. Произвести настройку с соответствия точек прохода и параметров внешних систем (выполняется во внешних системах).
6. Настроить СКУД для двухфакторной аутентификации, если этот режим доступа используется.

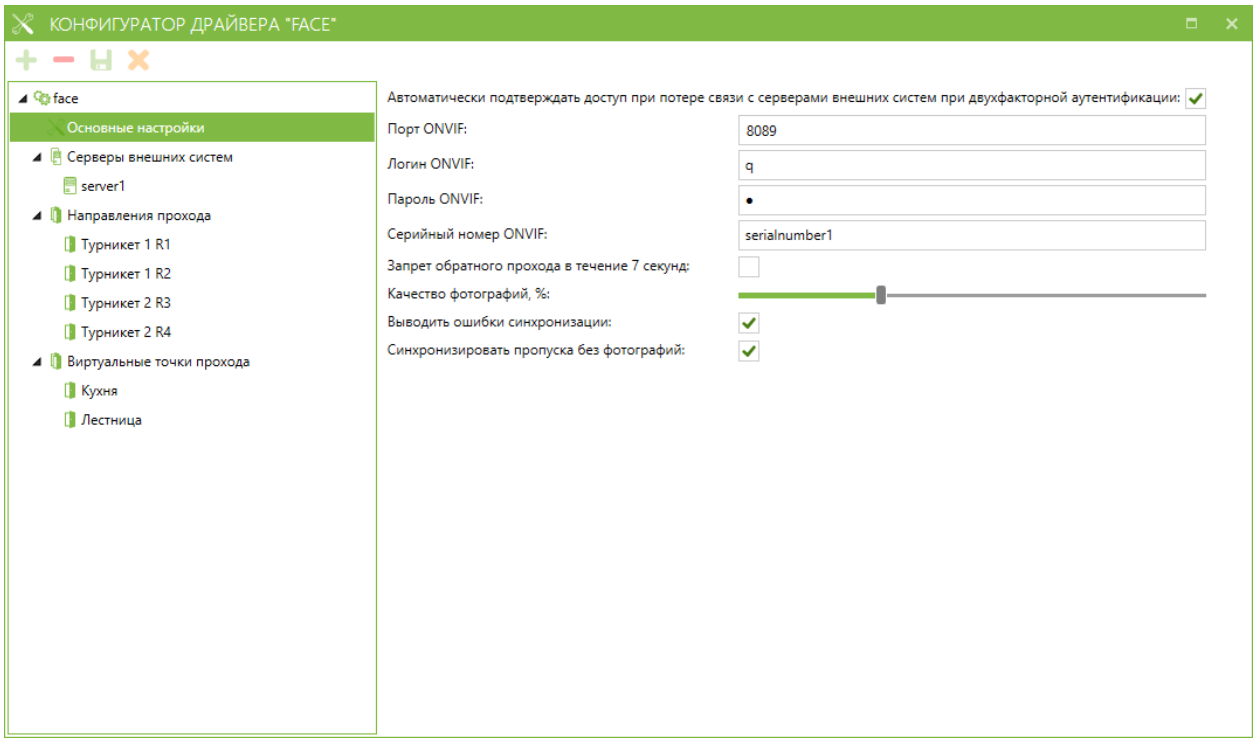

Рис. 1. Конфигуратор драйвера «Бастион-2 – Face»

4.2.1 Основные настройки

В основных настройках определяются следующие параметры:

Автоматически подтверждать доступ при потере связи с серверами внешних систем при двухфакторной аутентификации (включено по умолчанию) – при включенной настройке, в случае потери связи драйвера «Бастион-2 – Face» с внешней системой, драйвер будет выдавать автоматическое подтверждение доступа для всех карт, по которым такое подтверждение будет запрошено. Если настройка отключена, то при отсутствии связи с внешней системой 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 АПК «Бастион-2» 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 внешних серверов.

Серийный номер ONVIF – это поле нужно заполнить серийным номером АПК «Бастион-2».

Запрет обратного прохода в течение 7 секунд – при включении этой опции доступ не будет предоставляться, если посетитель попытается выйти на том же направлении прохода в течение 7 секунд после входа или войти в течение 7 секунд после выхода.

Качество фотографий, % – качество сжатия изображений с видеокамер, передаваемых из внешних систем 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 идентификации и аутентификации,
2. Сохранения в журнал событий АПК «Бастион-2» 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.

4.2.2 Настройка соединений с серверами внешних систем

Узел дерева настроек «Серверы внешних систем» группирует настроенные подключения к серверам внешних систем. Для добавления нового сервера следует нажать кнопку «Добавить» на панели инструментов конфигуратора, для удаления – кнопку «Удалить». Настройки подключения к серверу 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.

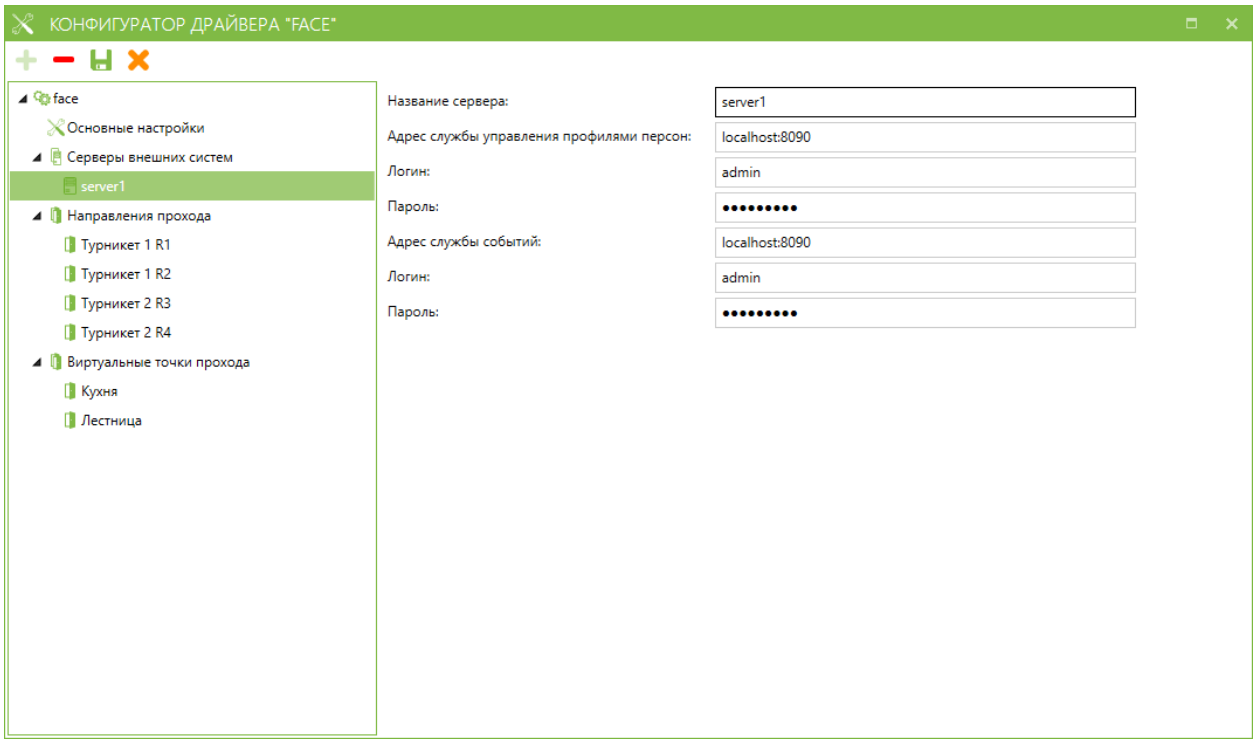

Рис. 2. Настройки подключения к серверу внешней системы

4.2.3 Направления прохода

Узел конфигурации «Направления прохода» содержит считыватели СКУД, подключенные к внешней системе. Для подключения считывателей следует выделить узел настроек «Направления прохода» и нажать кнопку «Добавить» на панели инструментов, в результате чего откроется окно добавления считывателей (Рис. 3). Для отключения считывателя от внешней системы следует выделить его в дереве конфигурации и нажать кнопку «Удалить».

Настройка соответствия считывателей и внешних датчиков (например, видеокамер внешней системы) должно производиться в модуле конфигурации внешней системы.

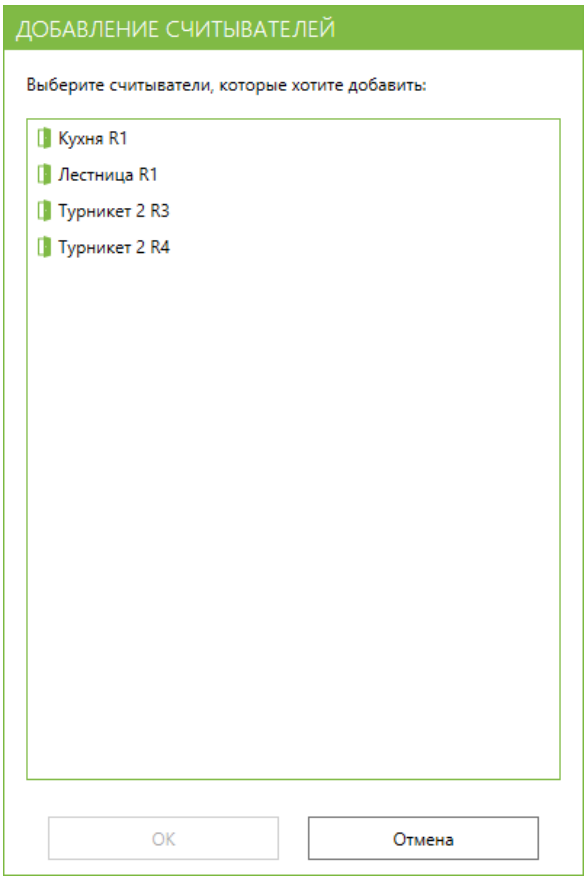

Рис. 3. Добавление считывателей

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 внешней системы. Рекомендуется указывать здесь примерное описание местоположения считывателя.

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

Доступ только по карте – в этом режиме считыватель будет работать без использования внешней 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 во внешней системе (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 выполняет собственные проверки и выдает подтверждение / отказ в доступе.

4.2.4 Настройка СКУД для двухфакторной аутентификации

Для обеспечения работы направления прохода совместно с внешней системой 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. 5). Для получения информации о настройке СКУД ELSYS следует ознакомиться с документом «Бастион-2 – ELSYS. Руководство администратора».

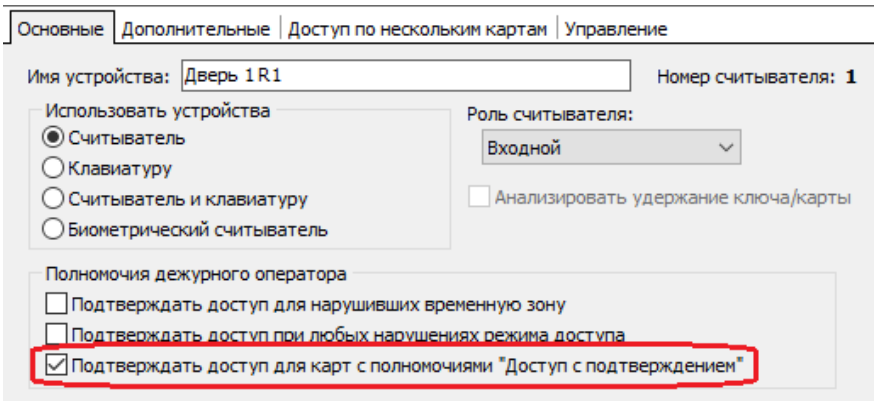

Рис. 5. Параметры направления прохода в настройках драйвера «Бастион-2 – ELSYS»

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

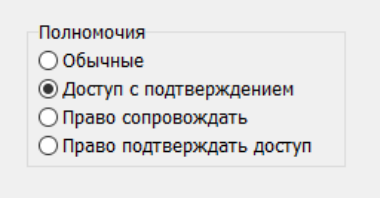

Рис. 6. Полномочия пропусков для доступа в режиме двухфакторной аутентификации

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 к внешней системе только в режиме двухфакторной аутентификации.*

4.2.5 Виртуальные точки прохода

Этот узел дерева настроек содержит виртуальные точки прохода. *Виртуальная точка прохода* не связана с реальным преграждающим устройством или считывателем, 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 двумя параметрами, представленными на Рис. 7.

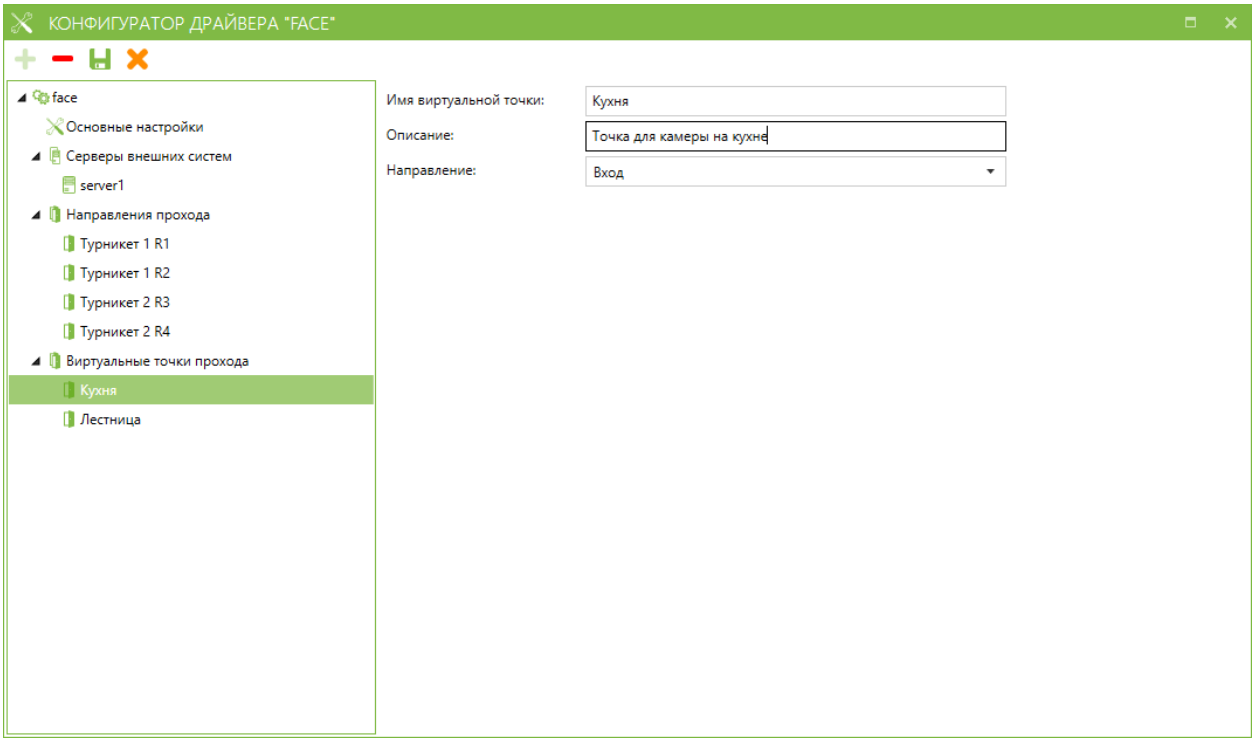

Рис. 7. Параметры виртуальной точки прохода

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.

5 Работа в штатном режиме

5.1 Синхронизация списка пропусков

Все выдаваемые в АРМ «Бюро пропусков» пропуска **с фотографией** синхронизируются с серверами внешних системы 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 АПК «Бастион-2» будет сгенерировано событие об ошибке синхронизации пропуска.*

При обновлении фотографии или ФИО владельца пропуска изменения отправляются автоматически на сервера внешних систем. В случае, если это по каким-либо причинам не произошло, для обновления фотографии на серверах внешних систем необходимо в АРМ Бюро пропусков в контекстном меню пропуска выбрать пункт «Обновить пропуск в контроллерах» (Рис. 8).

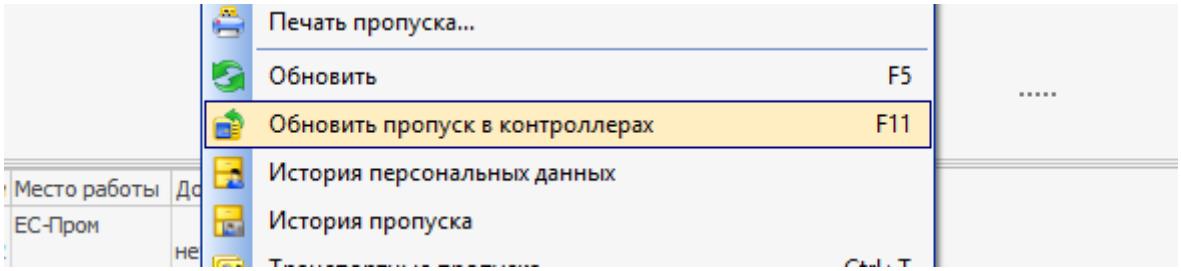

Рис. 8. Обновление данных пропуска на серверах внешних систем

В случае, если идентификация пользователя СКУД по фотографии из АПК «Бастион-2» происходит с низкой вероятностью, то следует произвести настройки внешней системы (снизить порог распознавания, добавить дополнительные фотографии). Подробно об этих операциях см. Руководство по внешней системе.

5.2 Режим двухфакторной аутентификации

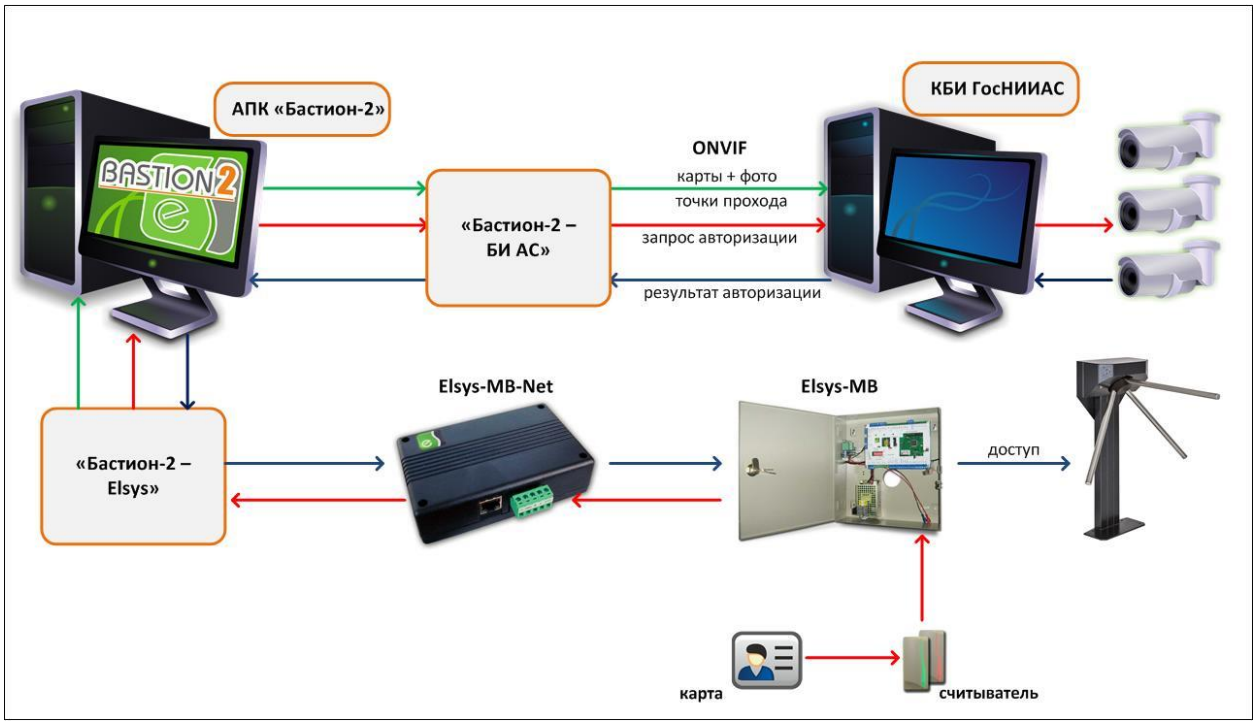

Рис. 9. Работа системы в режиме двухфакторной аутентификации

В режиме двухфакторной аутентификации посетитель сначала прикладывает пропуск к считывателю. При этом его лицо должно быть в зоне обзора камеры видеонаблюдения, которая контролирует направление доступа. 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 на сервера внешних систем модулем «Бастион-2 – 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-2 – Face» и драйвер «Бастион-2 – ELSYS» в контроллер (Рис. 9).

Если лица не соответствуют (посетитель прикладывает карту доступа, выданную не ему), то доступ предоставлен не будет. В «Бастион-2» 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-2» 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-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 внешних систем. 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

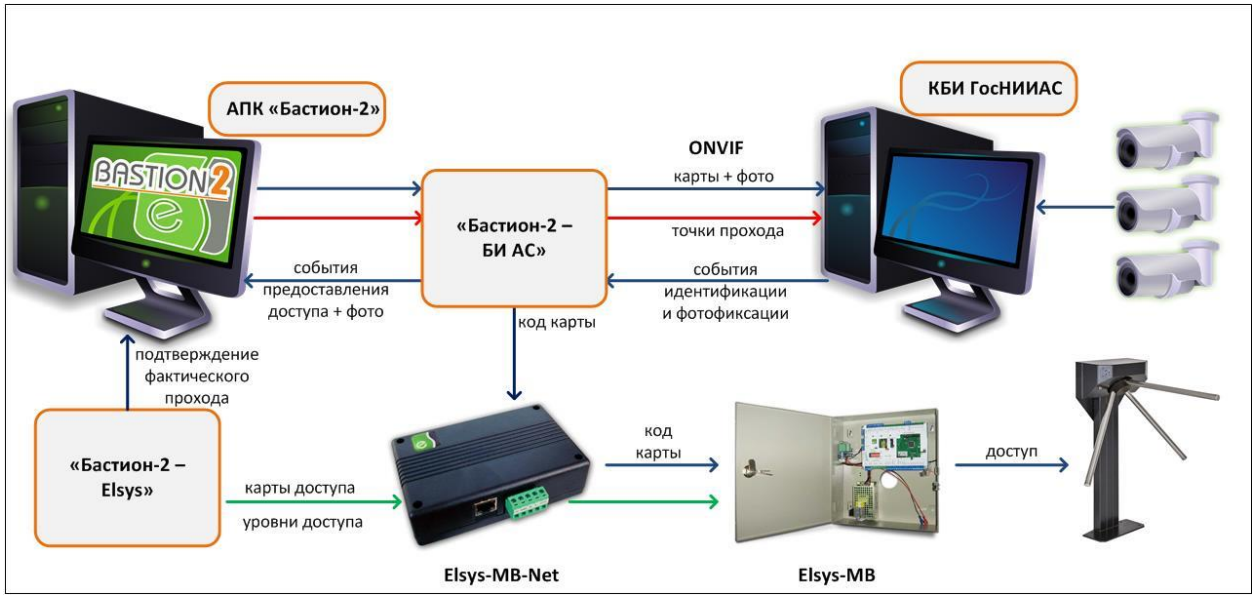

Рис. 10. Работа системы в режиме идентификации

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. 10).

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-2» 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-2» 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-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 направлении прохода в обратном направлении в течение 7 секунд после прохода. В «Бастион-2» 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

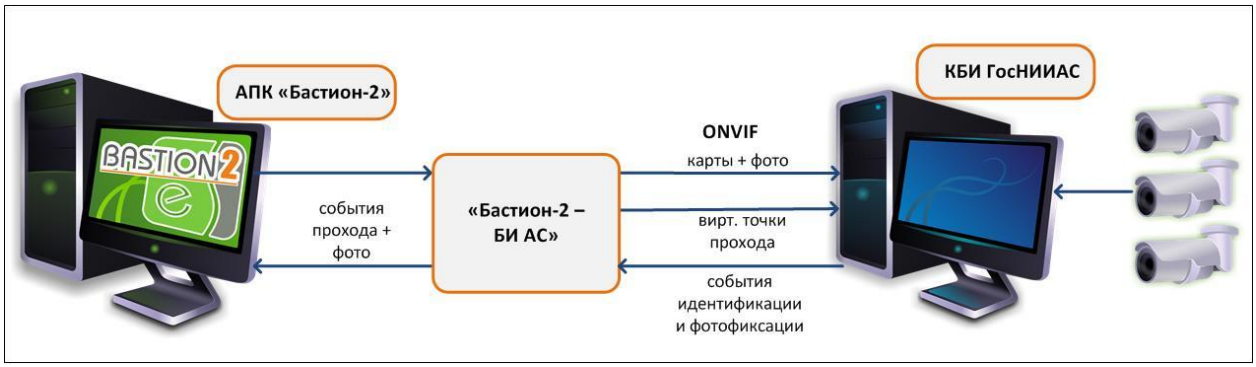

Рис. 11. Работа системы с виртуальными точками прохода

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

Если внешняя система обнаружит в системе активный пропуск, имеющий фотографию лица, совпадающего с лицом на изображении, полученного с камеры видеонаблюдения, то в «Бастион-2» будет сгенерировано событие **«Штатный проход *<ФИО посетителя>*»**.

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-2» будет сгенерировано тревожное событие **«Проход неизвестного лица»**.

В обоих случаях к генерируемому событию будет прикреплено изображение посетителя, полученное с камеры видеонаблюдения. Если соответствующая настройка включена в параметрах «Бастион-2», 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-2» 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 АПК «Бастион-2» и серверов внешней системы. В случае неисправности хотя бы одного из компонентов, подтверждение доступа для карт передаваться не будет и в доступе будет отказано. 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.
Считыватель	Штатный вход %s1	Для виртуальных точек прохода, настроенных, как вход, возникает при обнаружении известного лица в зоне обзора соответствующей камеры.
Считыватель	Штатный выход %s1	Для виртуальных точек прохода, настроенных, как выход, возникает при обнаружении известного лица в зоне обзора соответствующей камеры.
Считыватель	Вход неизвестного лица	Для виртуальных точек прохода, настроенных, как вход, возникает при обнаружении неизвестного лица в зоне обзора соответствующей камеры.
Считыватель	Вход неизвестного лица	Для виртуальных точек прохода, настроенных, как выход, возникает при обнаружении неизвестного лица в зоне обзора соответствующей камеры.

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 направлении прохода в обратном направлении в течение 7 секунд после прохода.
Виртуальное устройство 1	В доступе отказано (попытка прохода по фото). %s2	При обнаружении сервером внешней системы 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

1.1.3 (25.05.2026)

[*] События прохода на виртуальных точках прохода Face теперь отображаются на форме настроек персонала.

[*] Если включена функция автоматического возврата неактивных пропусков, то больше не выполняется автоматический возврат пропусков, у которых имеются проходы по виртуальным точкам прохода Face.

1.1.2 (31.12.2021)

[+] Возможность работы не только с драйвером «Бастион-2 – Elsys», но с любыми СКУД, интегрированными в АПК «Бастион-2».

[+] Используются новые оповещения о смене фотографии.

[+] Возможность настройки необходимости синхронизации пропусков, у которых не введена фотография.

[+] Виртуальные точки доступа теперь представлены и считывателем, и дверью, что позволяет использовать их в уровнях доступа и в областях контроля.

1.1.1 (19.03.2021)

[*] Драйвер переименован в «Бастион-2 – Face».

[*] Удалён профиль персонала для драйвера, так как он не используется.

[*] Обновлена документация, добавлены приложения со списком событий и историей изменений.

1.1.0 (01.12.2020)

[+] Добавлена возможность принимать с сервера внешней системы признаки наличия маски и значение измеренной температуры.

1.0.8 (20.03.2020)

[+] Добавлена возможность отключить генерацию событий при ошибках синхронизации пропусков.

[+] Версия включена в комплект поставки АПК «Бастион-2».