Бастион-2 – Face. Руководство администратора

Версия 1.1.1

(19.03.2021)

Самара, 2021

Оглавление

1 Общие сведения

1.1 Назначение и область применения

Модуль «Бастион-2 – Face» предназначен для подключения к АПК «Бастион-2» комплексов биометрической идентификации (КБИ) сторонних производителей. Взаимодействие с КБИ производится с использованием протокола на основе стандарта ONVIF Profile A, C.

Интеграция может быть выполнена силами производителей КБИ. 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 АПК «Бастион-2».

Модуль позволяет использовать как режим двухфакторной авторизации (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 КБИ.

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 (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 авторизации.

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 авторизации.

Для обмена данными между модулем «Бастион-2 – Face» и КБИ используется протокол ONVIF Profile A, C.

Модуль совместим 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 авторизации 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 самого КБИ.

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 КБИ.
3. Добавить точки прохода и определить режимы доступа для них.
4. Добавить необходимые виртуальные точки прохода.
5. Настроить соответствия точек прохода и видеокамер (выполняется в КБИ).
6. Настроить СКУД для двухфакторной авторизации, если этот режим доступа используется.

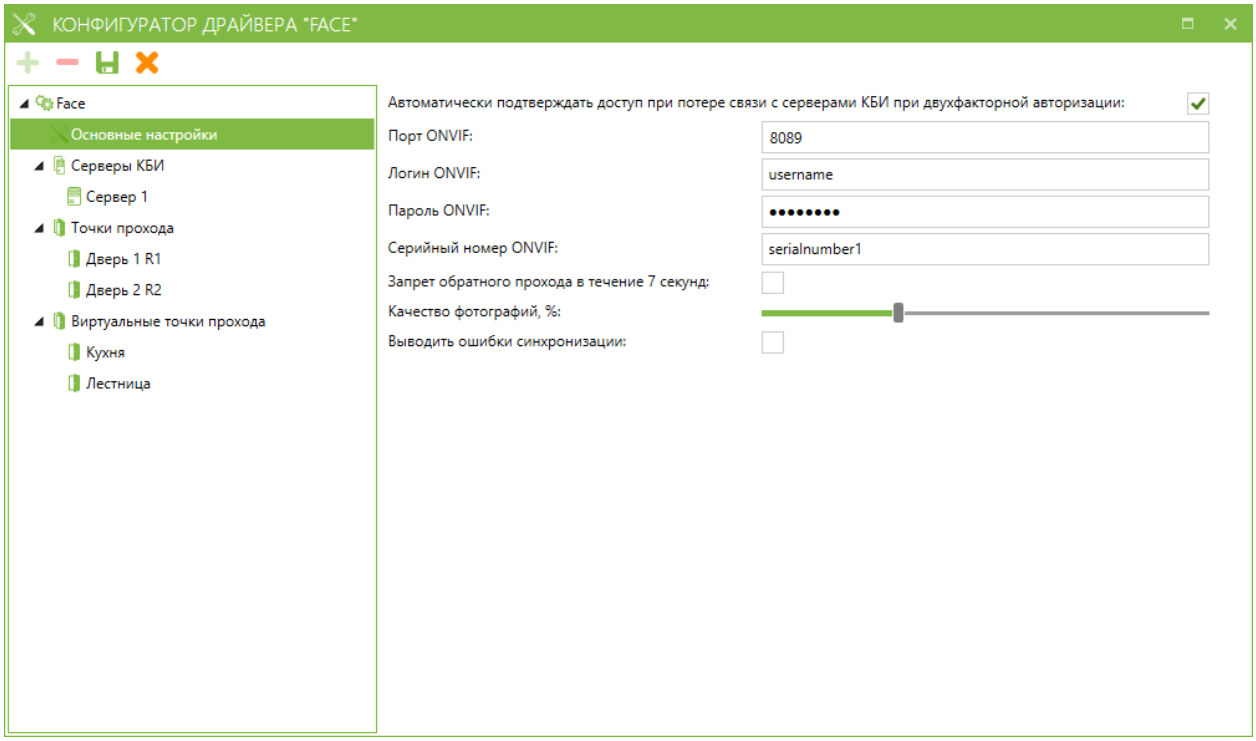

Рис. 1. Конфигуратор драйвера «Бастион-2 – Face»

4.2.1 Основные настройки

В основных настройках определяются следующие параметры:

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

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 (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 КБИ в АПК «Бастион-2» при событиях прохода. Следует иметь ввиду, что эти фотографии используются для:

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

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 КБИ

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

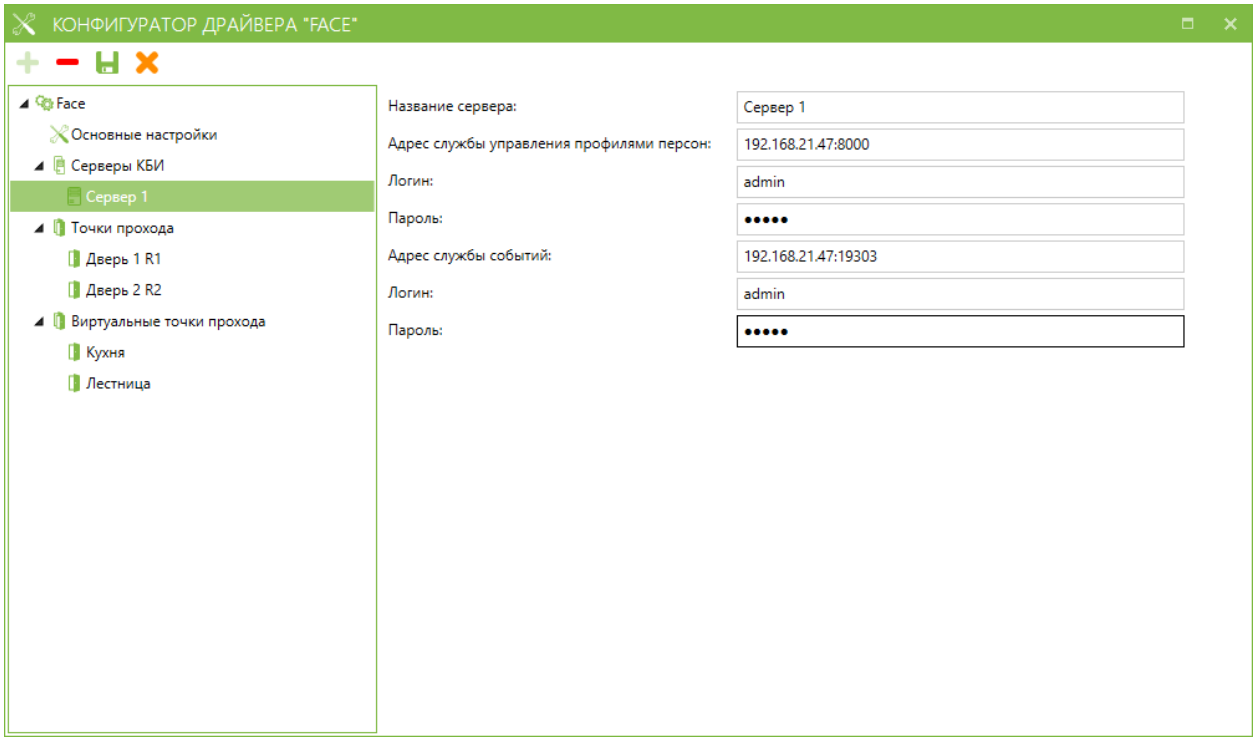

Рис. 2. Настройки подключения к серверу КБИ

4.2.3 Точки прохода

Узел конфигурации «Точки прохода» группирует точки прохода СКУД, подключенные к КБИ. Для подключения точек прохода следует выделить узел настроек «Точки прохода» и нажать кнопку «Добавить» на панели инструментов, в результате чего откроется окно добавления точек прохода (Рис. 3). Для отключения точки прохода от КБИ необходимо выделить точку в дереве конфигурации и нажать кнопку «Удалить».

В рамках драйвера «Бастион-2 – Face» каждой точке прохода соответствует считыватель СКУД ELSYS. Настройка соответствия точек прохода и видеокамер КБИ должно производиться в модуле конфигурации самого КБИ.

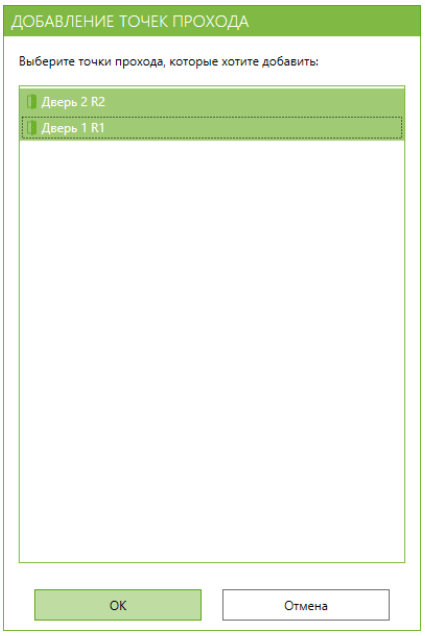

Рис. 3. Добавление точек прохода

Настройки подключенной точки прохода (Рис. 4) представлены двумя параметрами, которые описаны ниже.

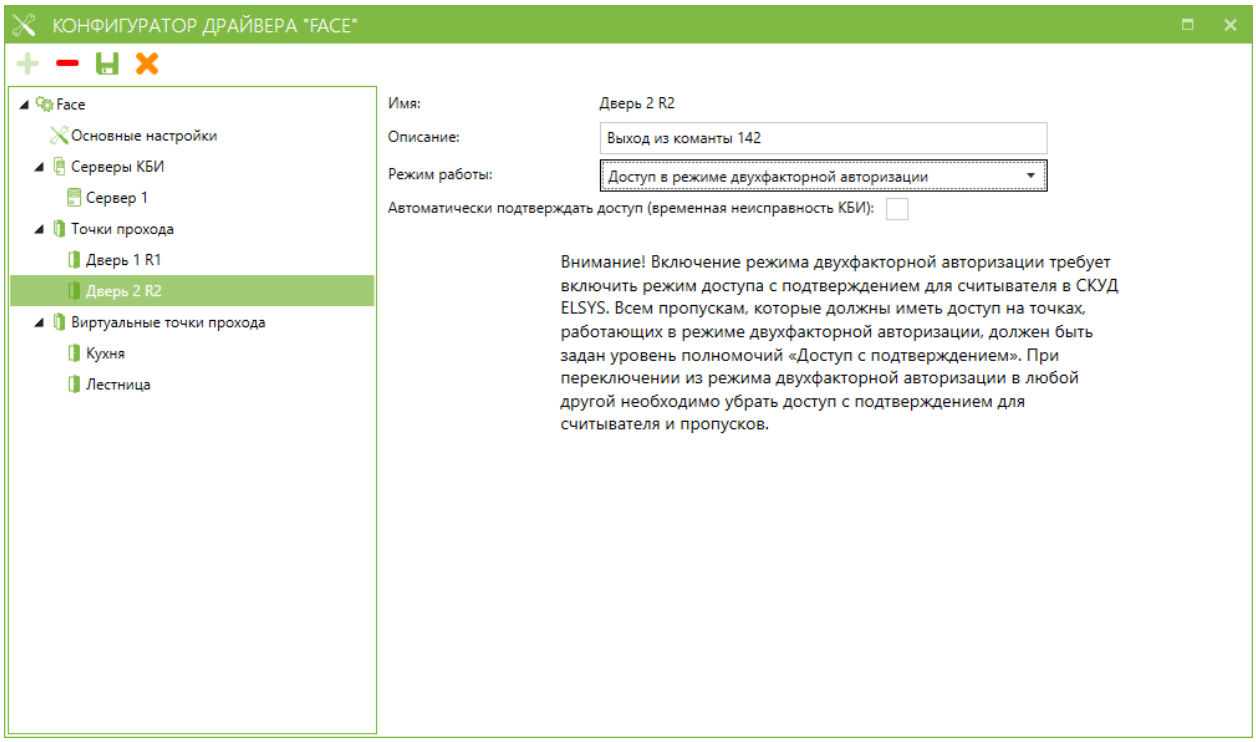

Рис. 4. Параметры точки прохода

Описание – текстовое описание, комментарий к точке прохода. Передаётся на серверы КБИ. Описание служит для облегчения идентификации точки прохода при настройке связей камер видеонаблюдения с точками прохода СКУД при конфигурировании КБИ. Значение настройки должно содержать примерное описание местоположения точки прохода.

Режим работы – определяет режим предоставления доступа для выбранной точки 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 авторизации – в этом режиме посетитель сначала прикладывает карту к считывателю, затем сервер КБИ сопоставляет изображение, полученное с привязанной камеры, с фотографией посетителя, которая сохранена в «Бастион-2», и выдает подтверждение / отказ в доступе.

Автоматически подтверждать доступ (временная неисправность КБИ) – опцию следует включать в режиме двухфакторной авторизации только в том случае, если необходимо временно отключить подтверждение доступа через КБИ, то есть – в случае временной неисправности КБИ. Если опция включена, драйвер «Бастион-2 – Face» будет самостоятельно давать подтверждение всем картам, по которым оно будет запрашиваться, не отправляя запрос в КБИ. Настройка позволяет не отключать доступ с подтверждением для пропусков и считывателей, отключив временно фактический запрос подтверждения через КБИ.

4.2.4 Настройка СКУД для двухфакторной авторизации

Для обеспечения работы точки прохода совместно с КБИ в режиме двухфакторной авторизации 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».

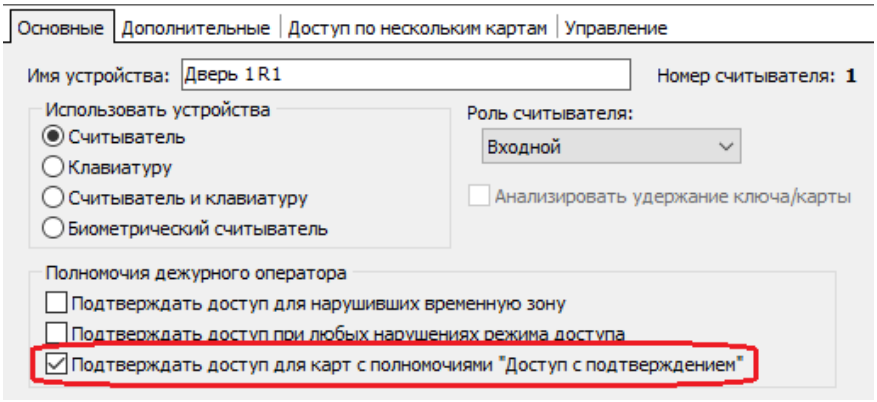

Рис. 5. Параметры точки прохода в настройках драйвера «Бастион-2 – ELSYS»

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

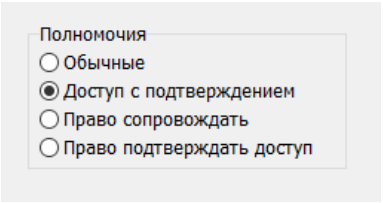

Рис. 6. Полномочия пропусков для доступа в режиме двухфакторной авторизации

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). Точки прохода контроллеров ELSYS MB-IP можно подключать к КБИ только в режиме двухфакторной авторизации.*

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 к КБИ.

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.

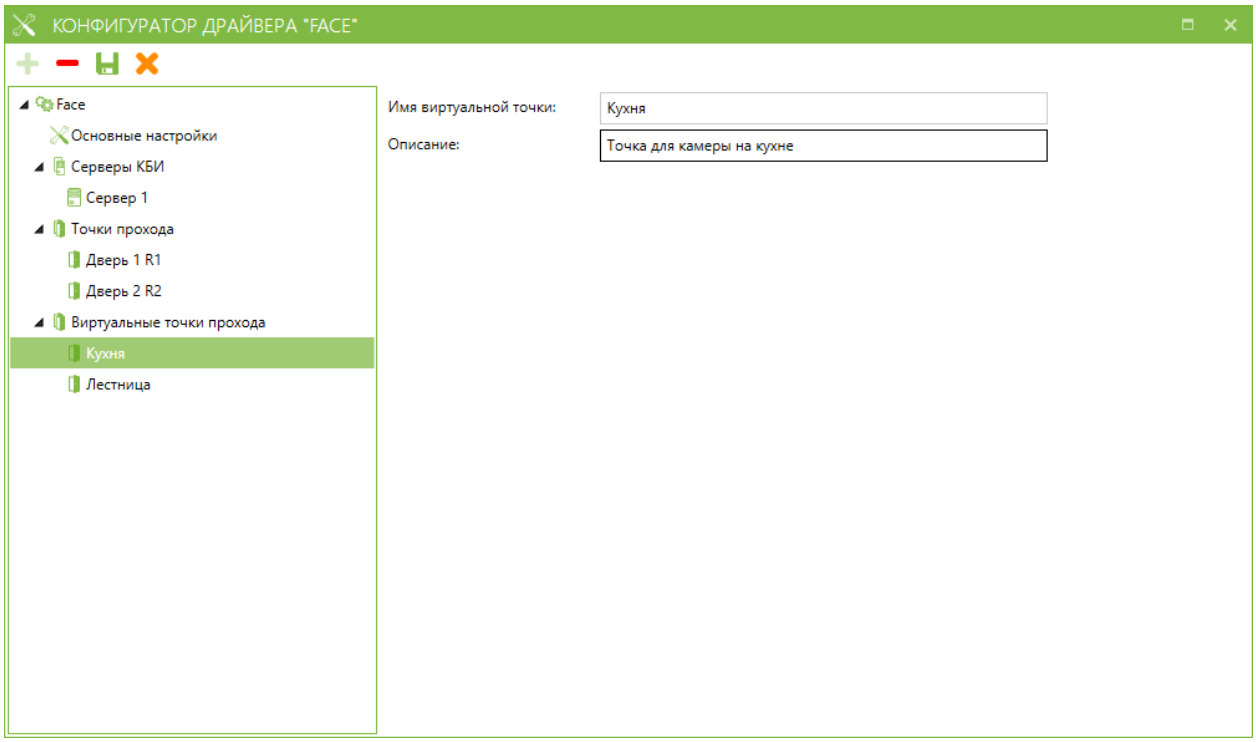

Рис. 7. Параметры виртуальной точки прохода

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

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

5 Работа в штатном режиме

5.1 Синхронизация списка пропусков

Все выдаваемые в АРМ «Бюро пропусков» пропуска **с фотографией** синхронизируются с серверами КБИ в момент подключения к серверам КБИ.

> ***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 КБИ 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 КБИ. В случае, если это по каким-либо причинам не произошло, для обновления фотографии на серверах КБИ необходимо в АРМ Бюро пропусков в контекстном меню пропуска выбрать пункт «Обновить пропуск в контроллерах» (Рис. 8).

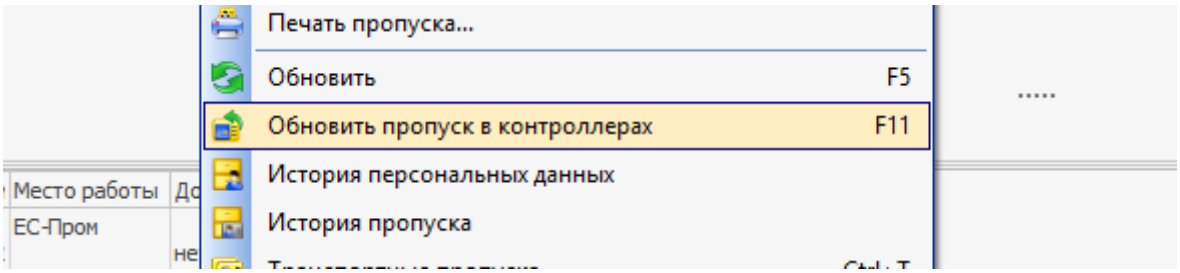

Рис. 8. Обновление данных пропуска на серверах КБИ

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

5.2 Режим двухфакторной авторизации

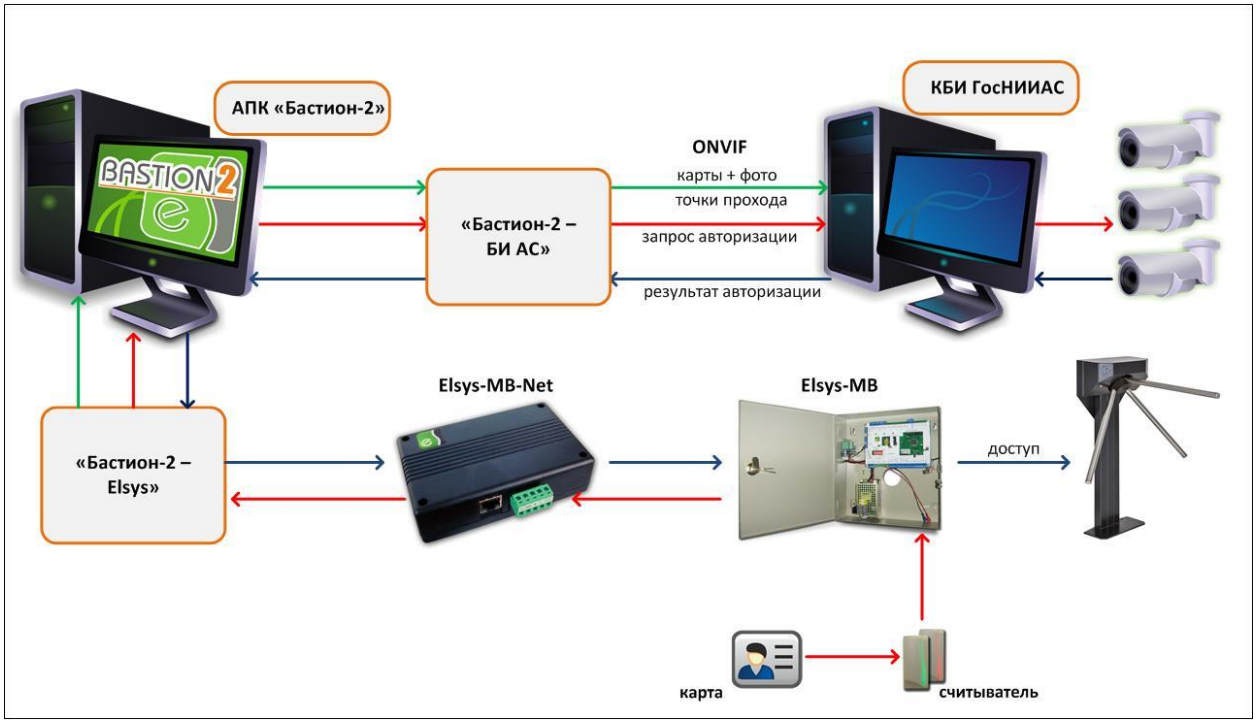

Рис. 9. Работа системы в режиме двухфакторной авторизации

В режиме двухфакторной авторизации посетитель сначала прикладывает пропуск к считывателю. При этом его лицо должно быть в зоне обзора камеры видеонаблюдения, которая контролирует точку доступа. Контроллер Elsys-MB проверяет права предъявленной карты доступа. Если для карты активна опция «Доступ с подтверждением», то контроллер выдает запрос внешней авторизации карты, который передается в КБИ модулем «Бастион-2 – Face». КБИ 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 авторизации передается обратно от КБИ, 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 точки 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 точки 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 авторизации требует наличия связи и работоспособности не только контроллеров ELSYS, но и модулей АПК «Бастион-2» и КБИ. В случае неисправности хотя бы одного из компонентов, подтверждение доступа для карт передаваться не будет и в доступе будет отказано. В случае неисправности КБИ рекомендуется для соответствующих точек прохода временно устанавливать опцию «Автоматически подтверждать доступ (Временная неисправность КБИ)». Также, рекомендуется всегда включать опцию «Автоматически подтверждать доступ при потере связи с КБИ при двухфакторной авторизации».*

5.3 Режим идентификации

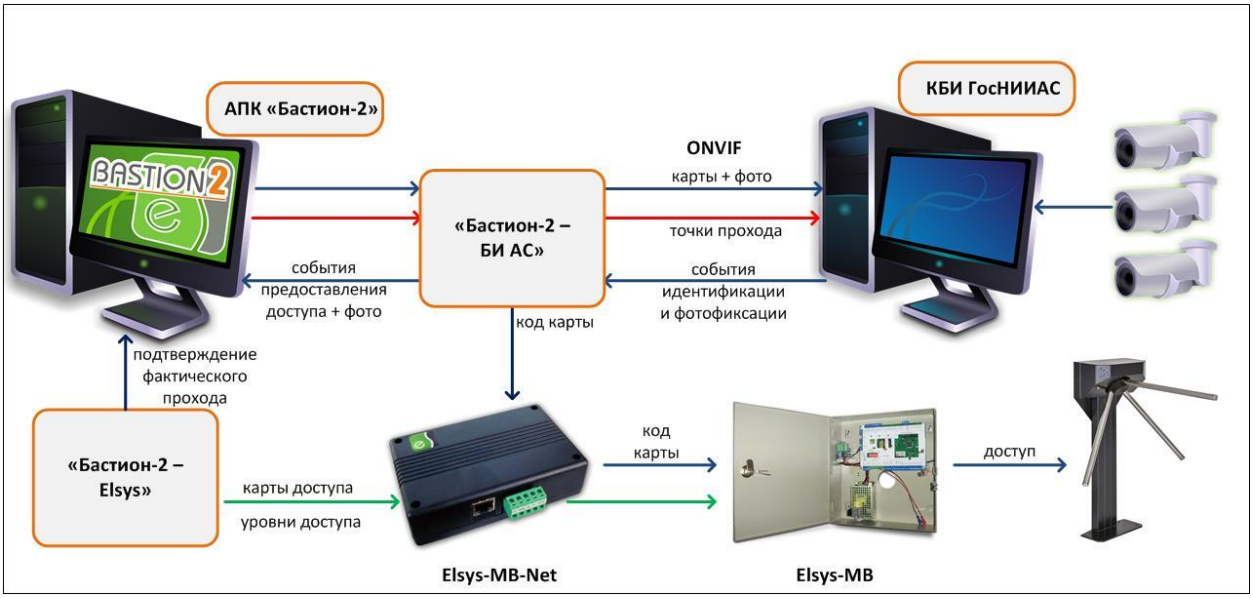

Рис. 10. Работа системы в режиме идентификации

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 точке прохода посетителю достаточно встать напротив камеры видеонаблюдения. КБИ проанализирует изображение лица посетителя, полученное с камеры, и сравнит его с фотографиями всех активных пропусков, существующих в системе (Рис. 10).

Если КБИ 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>:* 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 точки 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 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

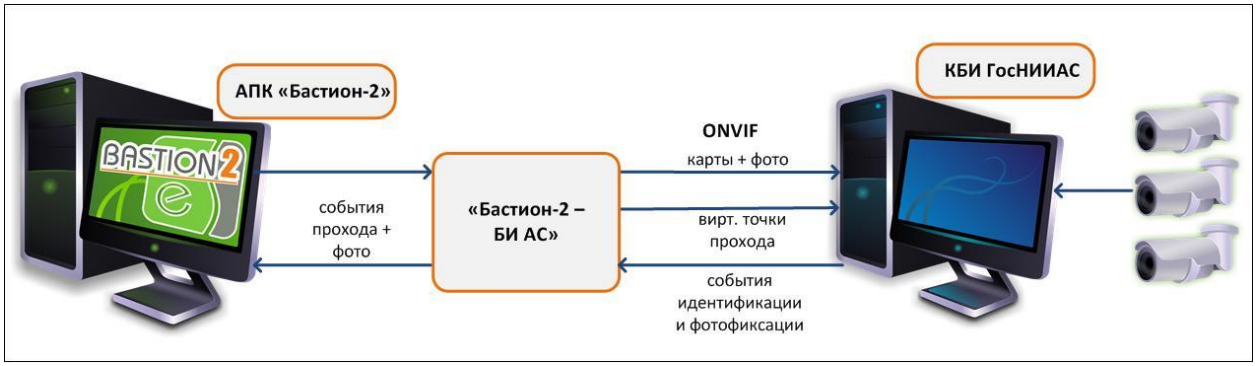

Рис. 11. Работа системы с виртуальными точками прохода

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

Если КБИ 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 используемого КБИ, 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 точки 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 КБИ.

6 Нештатные ситуации

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

Режим двухфакторной авторизации требует наличия связи и работоспособности не только контроллеров ELSYS, но и модулей АПК «Бастион-2» и КБИ. В случае неисправности хотя бы одного из компонентов, подтверждение доступа для карт передаваться не будет и в доступе будет отказано. В случае неисправности КБИ рекомендуется для соответствующих точек прохода временно устанавливать опцию «Автоматически подтверждать доступ (Временная неисправность КБИ)». Также, рекомендуется всегда включать опцию «Автоматически подтверждать доступ при потере связи с КБИ при двухфакторной авторизации».

В процессе синхронизации пропусков с сервером КБИ 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 КБИ: <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	Проход %s1	Для виртуальных точек прохода возникает при обнаружении известного лица в зоне обзора соответствующей камеры.
Считыватель	Проход неизвестного лица	Для виртуальных точек прохода возникает при

		обнаружении неизвестного лица в зоне обзора соответствующей камеры.
Сервер	Установлено соединение с сервером КБИ	При успешной установке связи с сервером КБИ
Сервер	Потеряно соединение с сервером КБИ	При потере связи с сервером КБИ
Сервер	%s1: не удалось синхронизировать пропуск с сервером КБИ: %s2	При ошибке синхронизации данных пропуска с сервером КБИ
Виртуальное устройство 1	Доступ подтверждён %s1. %s2	При успешном подтверждении доступа сервером КБИ в режиме двухфакторной авторизации
Виртуальное устройство 1	Доступ в режиме идентификации %s1. %s2	При предоставлении доступа сервером КБИ в режиме идентификации
Виртуальное устройство 1	В доступе отказано %s1. %s2"	При отказе в доступе сервером КБИ с указанием дополнительных признаков (маски, температуры)
Виртуальное устройство 1	В доступе отказано. %s2	При отказе в доступе сервером КБИ
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 устройство 1	В доступе отказано (попытка прохода по фото). %s2	При обнаружении сервером КБИ попытки прохода по фотографии вместо реального лица.
Виртуальное устройство 1	В доступе отказано %s1 (попытка прохода по фото). %s2	При обнаружении сервером КБИ попытки прохода по фотографии вместо реального лица с указанием дополнительных признаков.
Виртуальное устройство 1	Зафиксировано нарушение (%s2).	При обнаружении сервером КБИ 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 КБИ нарушений при проходе известного лица (например, «проход над турникетом» или «повышенная температура»), с указанием типа нарушения.

Приложение 2. История изменений

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 из КБИ 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».