



# Руководство по настройке и работе с модулем Виртуальный сервер доступа

ACFA-Интеллект

Обновлено 29/07/2024

## Содержание

<b>1</b>	<b>Введение в Руководство по настройке и работе с модулем Виртуальный сервер доступа .....</b>	<b>3</b>
1.1	Назначение документа.....	3
1.2	Общие сведения о программном модуле «Виртуальный сервер доступа».....	3
<b>2</b>	<b>Лицензирование модуля Виртуальный сервер доступа .....</b>	<b>4</b>
<b>3</b>	<b>Настройка программного модуля Виртуальный сервер доступа.....</b>	<b>5</b>
3.1	Настройка виртуальной точки прохода при распознавании номеров автомобилей.....	5
3.2	Настройка виртуальной точки прохода при распознавании лиц .....	7
3.3	Организация двухфакторной верификации .....	10
3.3.1	Общие сведения о двухфакторной верификации .....	10
3.3.2	Настройка двухфакторной верификации.....	11
	Настройка двухфакторной авторизации на стороне АСФА-Интеллект .....	11
	Настройка двухфакторной авторизации на стороне Face-Интеллект .....	16
3.4	Организация мониторинга и контроля температуры лица .....	16
3.4.1	Общие сведения о мониторинге и контроле температуры лица .....	16
3.4.2	Настройка системы мониторинга и контроля температуры лица .....	17
<b>4</b>	<b>Работа программного модуля Виртуальный сервер доступа .....</b>	<b>21</b>

# 1 Введение в Руководство по настройке и работе с модулем Виртуальный сервер доступа

## На странице:

- Назначение документа
- Общие сведения о программном модуле «Виртуальный сервер доступа»

## 1.1 Назначение документа

Документ *Руководство по настройке и работе с модулем «Виртуальный сервер доступа»* является справочно-информационным пособием и предназначен для специалистов по настройке программных комплексов *АСФА-Интеллект*, *Auto-Интеллект* и *Face-Интеллект*. В данном Руководстве представлены следующие материалы:

1. Общие сведения о модуле *Виртуальный сервер доступа*.
2. Настройка модуля *Виртуальный сервер доступа*.
3. Работа модуля *Виртуальный сервер доступа*.

## 1.2 Общие сведения о программном модуле «Виртуальный сервер доступа»

Программный модуль *Виртуальный сервер доступа* является частью программного комплекса *АСФА-Интеллект* и служит для объединения работы программных комплексов *Auto-Интеллект* и *Face-Интеллект* с *АСФА-Интеллект* путем создания виртуальных точек прохода (без оборудования СКУД).

Программный модуль *Виртуальный сервер доступа* позволяет выполнять следующие функции:

1. Создание виртуальных точек прохода (без оборудования СКУД) на базе распознавания лиц (см. [Настройка виртуальной точки прохода при распознавании лиц](#)) и номеров автомобилей (см. [Настройка виртуальной точки прохода при распознавании номеров автомобилей](#)).
2. В СКУД осуществлять двухфакторную верификацию в режиме Карта + Лицо (см. [Организация двухфакторной верификации](#)).
3. Выполнять мониторинг и контроль температуры лица, распознанного с помощью *Face-Интеллект* и тепловизора (см. [Организация мониторинга и контроля температуры лица](#)).
4. Выполнять различные действия в системе (например, открывать или закрывать шлагбаум, блокировать точку прохода) с помощью скриптов или макрокоманд по различным событиям (см. [Программный комплекс Интеллект. Руководство по программированию](#)).

Документация по программным комплексам *Auto-* и *Face-* и *Интеллект* базовый доступна [здесь](#).

## 2 Лицензирование модуля Виртуальный сервер доступа

Данный модуль не лицензируется.

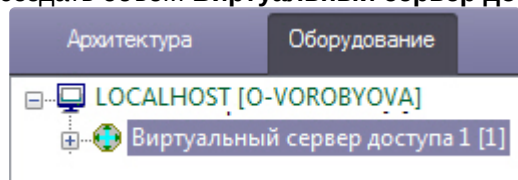
## 3 Настройка программного модуля Виртуальный сервер доступа

### 3.1 Настройка виртуальной точки прохода при распознавании номеров автомобилей

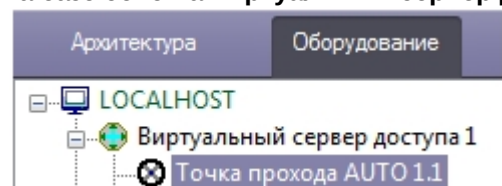
Организация виртуальной точки прохода при распознавании номеров автомобилей позволяет фиксировать проход (событие ACCESS\_IN) при распознавании номера, который есть в базе данных (в параметрах пользователя, задаваемых в модуле *Бюро пропусков*).

Для организации виртуальной точки прохода при распознавании номеров автомобилей необходимо выполнить следующие действия:

1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.



2. На базе объекта **Виртуальный сервер доступа** создать объект **Точка прохода AUTO**.



3. Выполнить настройку точки прохода:

4. Выбрать канал распознавания номеров, на базе которого необходимо организовать точку прохода (1).
5. Из раскрывающегося списка **Вход в** выбрать объект **Раздел** соответствующий территории, в которую осуществляется вход (2).
6. Из раскрывающегося списка **Выход из** выбрать объект **Раздел** соответствующий территории, из которой осуществляется выход (3).
7. Из раскрывающегося списка **Контроль** выбрать режим предоставления доступа (4):
  - **Решает сервер** - решение для доступа или отказа принимает сервер (в том числе при помощи скриптов).
  - **Решает оператор** - решение для доступа или отказа принимает оператор с помощью модуля *Диспетчер событий* (см. [Работа с программным модулем Диспетчер событий](#)). При выборе данного режима станут доступны следующие настройки:
 
    - **Таймаут** - задает в секундах временной интервал ожидания подтверждения доступа оператором. В течение заданного таймаута все прочие запросы от Канала распознавания номеров игнорируются.
8. Если был выбран режим предоставления доступа **Решает сервер**, то из раскрывающегося списка **Режим** (5) выбрать режим проверки прав доступа:

- **Только распознавание** – сервер принимает решение о предоставлении доступа только на основании распознавания номеров.
- **Проверка прав доступа** – сервер принимает решение о предоставлении доступа после успешного распознавания номера и успешной проверки прав доступа пользователя, которому принадлежит автомобиль (уровня доступа, временных зон, блокировки, двойного прохода). При выборе данного режима станут доступны следующие настройки:

Режим	Проверка прав доступа	▼
Начало действия	Не проверять	▼
Окончание действия	Не проверять	▼
Проверка блокировки		<input type="checkbox"/>
Проверка антипассбэка		<input type="checkbox"/>

- **Начало действия** и **Окончание действия** - задает режим проверки срока действия карты доступа:
  - **Не проверять** – не проверять дату начала или окончания срока действия карты.
  - **Не включительно** – не включать в проверку дату начала или окончания срока действия карты.
  - **Включительно** – включать в проверку дату начала или окончания срока действия карты.
- **Проверка блокировки** - установить флажок, чтобы проверять заблокирован ли пользователь.
- **Проверка антипассбэка** - установить флажок, чтобы осуществлять контроль двойного прохода.

9. Нажать кнопку **Применить (6)** для сохранения изменений.

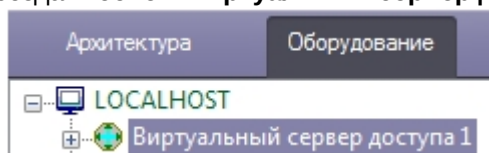
Организация виртуальной точки прохода при распознавании номеров автомобилей завершена.

## 3.2 Настройка виртуальной точки прохода при распознавании лиц

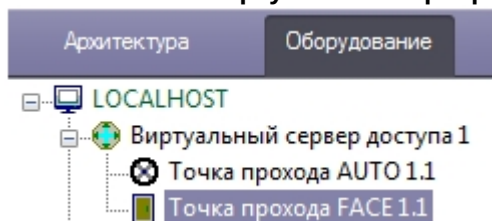
Организация виртуальной точки прохода при распознавании лиц позволяет фиксировать проход (событие ACCESS\_IN) при распознавании лица, которое есть в базе данных (см. [Программный комплекс Face-Интеллект. Руководство Администратора](#)).

Для организации виртуальной точки прохода при распознавании лиц необходимо выполнить следующие действия:

1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.



2. На базе объекта **Виртуальный сервер доступа** создать объект **Точка прохода FACE**.



3. Выполнить настройку точки прохода FACE:

4. Выбрать камеру, которой осуществляется распознавание лиц. Камера должна работать в составе сервера распознавания лиц (1).
5. Выбрать сервер распознавания лиц или канал распознавания, на базе которого необходимо организовать точку прохода (2).
6. Из раскрывающегося списка **Вход в** выбрать объект **Раздел** соответствующий территории, в которую осуществляется вход (3).
7. Из раскрывающегося списка **Выход из** выбрать объект **Раздел** соответствующий территории, из которой осуществляется выход (4).
8. Из раскрывающегося списка **Контроль** выбрать режим предоставления доступа (5):
  - **Решает сервер** - решение для доступа или отказа принимает сервер (в том числе при помощи скриптов).
  - **Решает оператор** - решение для доступа или отказа принимает оператор с помощью модуля *Диспетчер событий* (см. [Работа с программным модулем Диспетчер](#))



событий). При выборе данного режима станут доступны следующие настройки:

Контроль	Решает оператор
Таймаут	10

- **Таймаут** - задает в секундах временной интервал ожидания подтверждения доступа оператором. В течение заданного таймаута все прочие запросы от Сервера распознавания лиц игнорируются.
9. Если был выбран режим предоставления доступа **Решает сервер**, то из раскрывающегося списка **Режим** выбрать режим проверки прав доступа (**6**):
- **Только распознавание** – сервер принимает решение о предоставлении доступа только на основании распознавания лиц.
  - **Проверка прав доступа** – сервер принимает решение о предоставлении доступа после успешного распознавания лица и успешной проверки прав доступа пользователя (уровня доступа, временных зон, блокировки, двойного прохода). При выборе данного режима станут доступны следующие настройки:

Режим	Проверка прав доступа
Начало действия	Не проверять
Окончание действия	Не проверять
Проверка блокировки	<input type="checkbox"/>
Проверка антипассбэка	<input type="checkbox"/>

- **Начало действия и Окончание действия** - задает режим проверки срока действия карты доступа:
  - **Не проверять** – не проверять дату начала или окончания срока действия карты.
  - **Не включительно** – не включать в проверку дату начала или окончания срока действия карты.
  - **Включительно** – включать в проверку дату начала или окончания срока действия карты.
- **Проверка блокировки** - установить флажок, чтобы проверять заблокирован ли пользователь.
- **Проверка антипассбэка** - установить флажок, чтобы осуществлять контроль двойного прохода.
- **Мониторинг температуры** - если требуется осуществлять только мониторинг температуры лица (см. [Организация мониторинга и контроля температуры лица](#)).
- **Контроль температуры** - если требуется осуществлять только контроль превышения порога температуры лица (см. [Организация мониторинга и контроля температуры лица](#)). При выборе данного режима станут доступны следующие настройки:

Режим	Контроль температуры
Блокировка пользователя при тревоге	<input type="checkbox"/>

- **Блокировка пользователя при тревоге** - установить флажок, чтобы при превышении температуры пользователь автоматически блокировался (в модуле *Бюро пропусков* будет выставлен параметр **Пользователь заблокирован - Да**). При совместной работе со СКУД и включенной динамикой, такой пользователь будет автоматически удален из контроллера и, в результате, не получит доступ.
10. Нажать кнопку **Применить** (**7**) для сохранения изменений.

Организация виртуальной точки прохода при распознавании лиц завершена.

## 3.3 Организация двухфакторной верификации

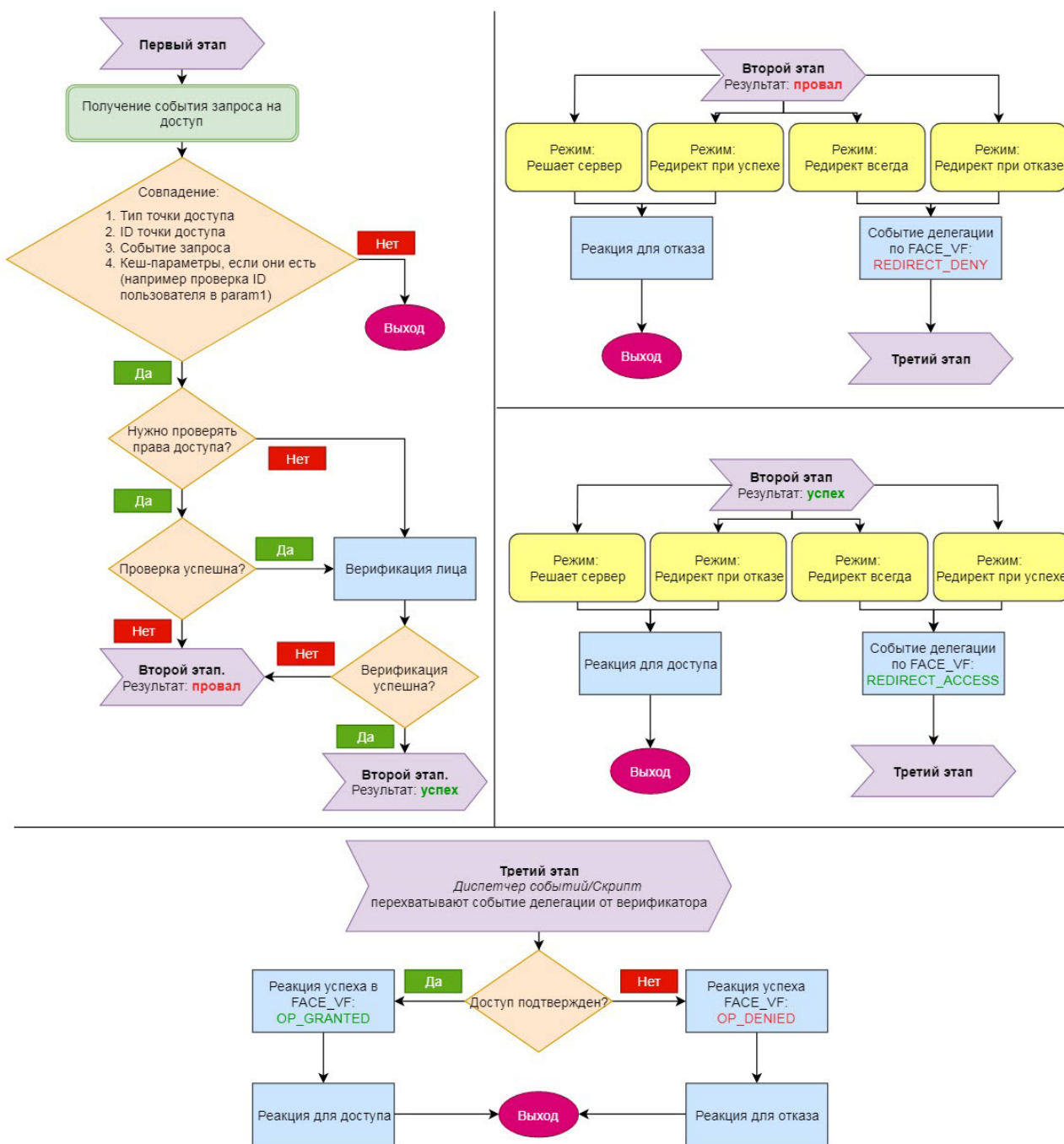
### 3.3.1 Общие сведения о двухфакторной верификации

Двухфакторная верификация позволяет в системах СКУД предоставлять доступ только после совместной успешной проверки Карты доступа пользователя и Лица данного пользователя.

 **Внимание!**

В этом режиме первой всегда должна прикладываться карта доступа пользователя и только затем происходит верификация лица.

Двухфакторная верификация происходит в несколько этапов. Блок схема работы двухфакторной верификации представлена ниже.



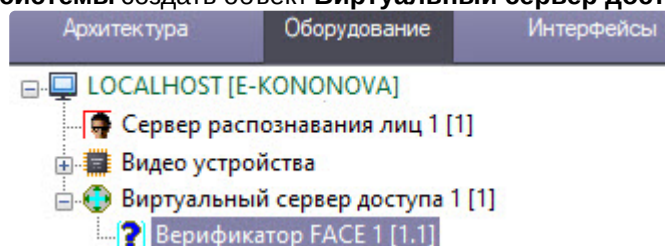
### 3.3.2 Настройка двухфакторной верификации

Организация двухфакторной авторизации включает в себя настройку на стороне АСФА-Интеллект и на стороне Face-Интеллект.

#### Настройка двухфакторной авторизации на стороне АСФА-Интеллект

Для настройки двухфакторной верификации необходимо выполнить следующие действия:

1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.



2. На базе объекта **Виртуальный сервер доступа** создать объект **Верификатор FACE**.
3. Перейти на его панель настройки.

4. На его настроечной панели из раскрывающегося списка **Камера** выбрать камеру, которая осуществляет захват лиц. Камера должна работать в составе **Сервера распознавания лиц** (см. [Настройка системного объекта Сервер распознавания лиц](#)).

5. Из раскрывающегося списка **Сервер** выбрать **Сервер распознавания лиц**.

6. Из раскрывающегося списка **Контроль** выбрать режим предоставления доступа:
  - **Решает сервер** – в зависимости от результата проверки прав доступа/верификации лица генерируется реакция для доступа или отказа.
  - **Редирект всегда** – независимо от результата второго этапа верификатор перенаправляет своё решение на внешний верификатор (*Диспетчер событий/Скрипт*). В зависимости от результата генерируется реакция для доступа или отказа.
  - **Редирект при отказе** – если первый этап успешен, то данный режим аналогичен режиму **Решает сервер**. Если первый этап провален, то осуществляется делегация внешнему верификатору.
  - **Редирект при успехе** – если первый этап провален, то данный режим аналогичен режиму **Решает сервер**. Если первый этап успешен, то осуществляется делегация внешнему верификатору.
7. Ввести значение поля **Таймаут** – время в секундах, по истечении которого связь с **Сервером распознавания лиц** разрывается.
8. При необходимости в полях группы **Кеш-параметры** задать параметры, индивидуальные для каждого программного модуля интеграции СКУД.

Кеш-параметры

param1

Генерировать собственное событие о предоставлении или отказе в доступе

**Примечание**

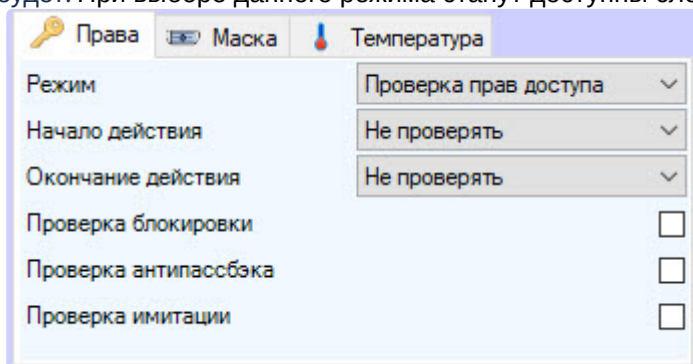
Например, в модуле интеграции *PERCo-S-20 v.2* каждый запрос оператору сопровождается параметром **request\_id**. Этот параметр необходимо обязательно возвращать при подтверждении доступа, иначе команда будет проигнорирована. Для СКУД *Hikvision* таким параметром является **param1**.

9. Установить флажок **Генерировать собственное событие о предоставлении или отказе в доступе**, чтобы дополнительное событие о предоставлении/отказе в доступе создавалось самим объектом **Верификатор FACE**, причем с указанием причины отказа. Данные события можно использовать для работы со скриптами или интерфейсным модулем *Диспетчер событий*.
10. Из раскрывающегося списка **Тип объекта** выбрать тип объекта, который будет являться инициатором проверки лица. Как правило, это точка доступа, считыватель и т.п.

Тип объекта:	Считыватель Hikvision 26X
Объект:	Считыватель Hikvision 26X 1
Событие:	Лицо не существует
Реакция для доступа:	Открыть
Реакция для отказа:	Оставить закрытой

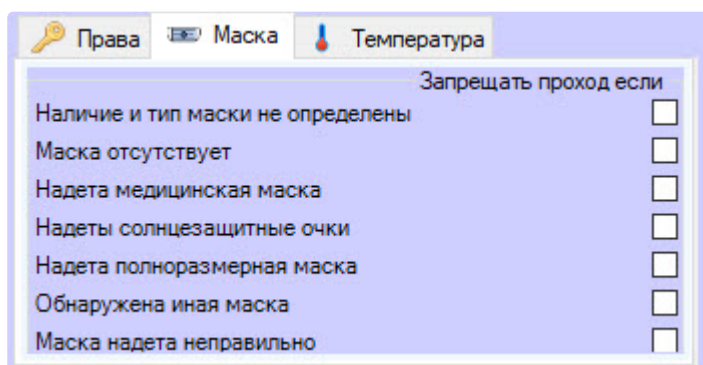
11. Из раскрывающегося списка **Объект** выбрать объект заданного выше типа.
12. Из раскрывающегося списка **Событие** выбрать событие, по которому будет запущена проверка лица. Список доступных событий зависит от выбранного типа объекта.

13. Из раскрывающегося списка **Реакция для доступа** выбрать команду, которая будет отправлена на объект-инициатор при успешной верификации лица. Список доступных команд зависит от выбранного типа объекта.
14. Из раскрывающегося списка **Реакция для отказа** выбрать команду, которая будет отправлена на объект-инициатор при неуспешной проверке/верификации лица. Список доступных команд зависит от выбранного типа объекта.
15. На вкладке **Права** из раскрывающегося списка **Режим** выбрать режим проверки прав доступа:
  - a. **Только распознавание** – сервер принимает решение о предоставлении доступа только на основании верификации лица.
  - b. **Проверка прав доступа** – сервер принимает решение о предоставлении доступа после успешной проверки прав доступа пользователя (уровня доступа, временных зон, блокировки, отсутствия двойного прохода) и затем успешной верификации лица. Если на этапе проверки прав доступа будет обнаружено несоответствие прав, то на устройство будет выдан отказ в доступе, а верификация лица запущена не будет. Событие об отказе в доступе от объекта **Верификатор FACE** в *Протоколе событий* отображаться не будет. При выборе данного режима станут доступны следующие настройки:

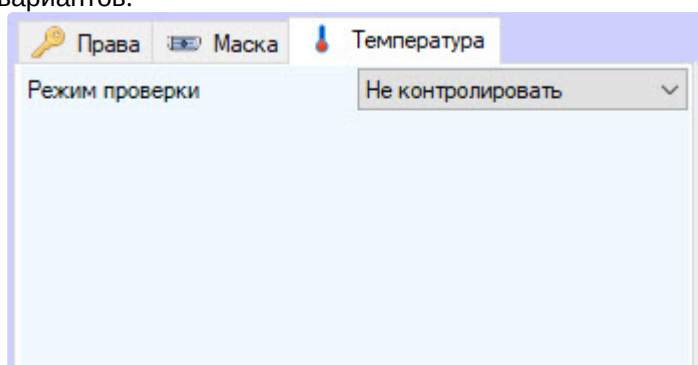


- i. **Начало действия** и **Окончание действия** – задается режим проверки срока действия карты доступа:
        - **Не проверять** – не проверять дату начала или окончания срока действия карты:
        - **Не включительно** – не включать в проверку дату начала или окончания срока действия карты:
        - **Включительно** – включать в проверку дату начала или окончания срока действия карты.
      - ii. **Проверка блокировки** – установить флажок, чтобы проверять, заблокирован ли пользователь.
      - iii. **Проверка антипассбэка** – установить флажок для контроля двойного прохода.
      - iv. **Проверка имитации** – установить флажок для контроля предъявления фотографии лица вместо живой персоны. По умолчанию флажок снят.
16. Перейти на вкладку **Маска** и установить флажки **Запрещать проход если**, чтобы высылался запрет доступа в зависимости от выставленных флажков. Если в данном блоке настроек не выставить ни один флажок, то распознавание маски будет игнорироваться.

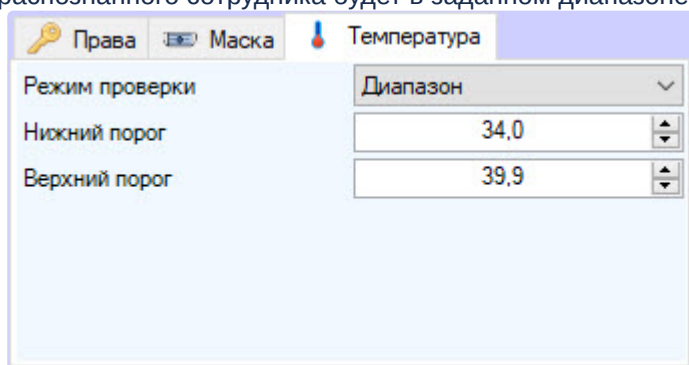


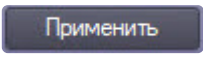


17. Перейти на вкладку **Температура** и из выпадающего списка **Режим проверки** выбрать один из вариантов:



- **Не контролировать** – независимо от температуры у распознанного пользователя доступ будет разрешен.
- **Превышение порога** – запрет доступа при температурном пороге, который задается в **Сервере распознавания лиц** на вкладке **Аналитика** (подробнее см. [Панель настройки системного объекта Сервер распознавания лиц](#)).
- **Диапазон** – в полях **Нижний порог** и **Верхний порог** указать минимально и максимально допустимую температуру соответственно. Доступ разрешен, если температура распознанного сотрудника будет в заданном диапазоне.



18. Нажать кнопку **Применить**  для сохранения настроек.

Пример настройки двухфакторной верификации для модуля интеграции СКУД *Hikvision* представлен ниже.

Настройка двухфакторной верификации на стороне АСФА-Интеллект завершена.

### Настройка двухфакторной авторизации на стороне Face-Интеллект

Для работы двухфакторной верификации не требуется база лиц.

На стороне Face-Интеллект нужно:

1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Сервер распознавания лиц**.
2. На базе объекта **Сервер распознавания лиц** создать объекты **Канал распознавания** и **Модуль распознавания Tevian**.

Настройка двухфакторной верификации на стороне Face-Интеллект завершена.

## 3.4 Организация мониторинга и контроля температуры лица

### 3.4.1 Общие сведения о мониторинге и контроле температуры лица

Программный модуль **Виртуальный сервер доступа** позволяет получать температуру лица, которую замеряет тепловизор на стороне ПК Face-Интеллект при распознавании лица. Температуру лица, например, можно отображать на мониторе для Оператора с помощью программного



модуля *Диспетчер событий* и, в случае превышения заданного порога температуры, заблокировать точку прохода до того момента, пока тревога не будет обработана Оператором.

### 3.4.2 Настройка системы мониторинга и контроля температуры лица

Настройка системы мониторинга и контроля температуры лица осуществляется следующим образом:

1. Выполнить настройку ПК *Face-Интеллект* согласно [документации](#).

✔ Настройка работы Сервера распознавания лиц с тепловизором.

2. Выполнить настройку объекта **Точка прохода FACE** согласно [документации](#). Обязательные настройки приведены ниже:
  - Если требуется осуществлять только мониторинг температуры (только отображение), то из раскрывающегося списка **Режим** выбрать **Мониторинг температуры**.
  - Если требуется осуществлять контроль превышения порога температуры, то из раскрывающегося списка **Режим** выбрать **Контроль температуры**.

**Примечание**

Для одновременной работы мониторинга и контроля температуры необходимо создать два объекта **Точка прохода FACE**, задав для каждого режим мониторинга/контроля температуры соответственно.

3. Выполнить настройку программного модуля *Диспетчер событий* согласно [документации](#). Обязательные настройки приведены ниже:

- а. Для каждого режима мониторинга/контроля создать и настроить объект **Правило отображения**:
  - Для параметра **Тип объекта** выбрать **Точка прохода FACE**.
  - Для параметра **Шаблон** выбрать шаблон отображения для мониторинга или контроля температуры соответственно (см. пункт 3.b).
  - На вкладке **Объекты** выбрать соответствующий объект **Точка прохода FACE** для мониторинга или контроля температуры.
  - На вкладке **События**, если настраивается объект **Правило отображения** для мониторинга температуры, установить флажок рядом с событием **Лицо распознано (лог температуры)**. Если настраивается объект **Правило отображения** для контроля температуры, то установить флажок рядом с событием **Распознано лицо с повышенной температурой**.
- б. Для каждого режима мониторинга/контроля создать и настроить объект **Шаблон отображения**:

✔ Свойства объекта **Поле БД**

- i. Для отображения названия события, на которое настроен *Диспетчер событий*, добавить объект **Поле БД**, указав в параметре **Нестандартное**:

rule\_service\_action\_name

- ii. Для отображения ФИО добавить несколько объектов **Поле БД**, указав в параметре **Предопределенное** поле из базы данных (Фамилия, Имя, Отчество), или добавить только один объект **Поле БД**, указав в параметре **Нестандартное**:

{param0}

- iii. Для отображения даты и времени, когда лицо и температура были распознаны, добавить объект **Поле БД**, указав в параметре **Нестандартное**:

{date} {time}

- iv. Для отображения температуры, полученной от тепловизора, добавить объект **Поле БД**, указав в параметре **Нестандартное**:

{temperature}

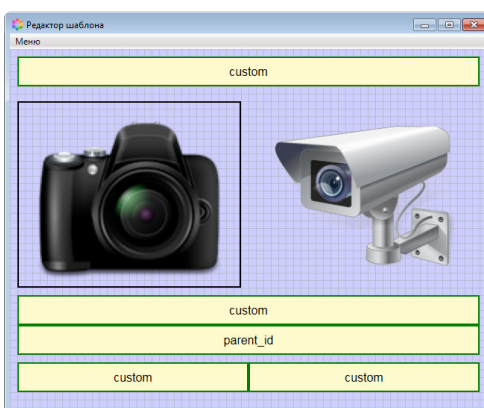
**Примечание**

Например, для шаблона контроля температуры, можно указать в параметре **Нестандартное**:

Внимание! Высокая температура: {temperature} °C {\n} Дверь заблокирована.

- v. Примеры шаблонов отображения приведены ниже.

**Шаблон отображения для мониторинга температуры**



**Шаблон отображения для контроля температуры**



4. В случае необходимости отображения захваченного лица с камеры от Сервера распознавания лиц, когда лицо распознать не удалось, выполнить настройку программного модуля *Диспетчер событий* согласно *документации*. Обязательные настройки приведены ниже:

- а. Создать и настроить новый объект **Правило отображения**:

- Для параметра **Тип объекта** выбрать **Сервер распознавания лиц**.
- Для параметра **Шаблон** выбрать шаблон отображения для нераспознанного лица (см. пункт 4.b).
- На вкладке **Объекты** выбрать соответствующий объект **Сервер распознавания лиц**.
- На вкладке **События** установить флажок рядом с событием **Не распознано**.

- b. Создать и настроить новый объект **Шаблон отображения**, в котором добавить объект **Фото пользователя**, указав в параметре **Параметр**:

imageBase64

✔ Свойства объекта Фото пользователя

Пример настроенной системы мониторинга и контроля температуры лица:

1. Режим мониторинга температуры:

Завоеванное лицо	Оптимизация ЭД	ФИО	Температура	Камера	Дата
		Голованова Юлия Анют	36,0	Камера главный вход	13.05.2020 17:15:58
		Голованова Юлия Анют	36,0	Камера главный вход	13.05.2020 17:15:59
		Голованова Юлия Анют	45,1%	Камера главный вход	13.05.2020 17:15:55
		Голованова Юлия Анют	57,7%	Камера главный вход	13.05.2020 17:15:45
		Голованова Юлия Анют	32,8%	Камера главный вход	13.05.2020 17:15:12
		Голованова Юлия Анют	37,0%	Камера главный вход	13.05.2020 17:15:05

**Внимание!**  
Голованова Юлия  
Температура: 36,0°

59%

Лицо распознано (лог температуры)

ФИО: Голованова Юлия. (36°С)

Ахилл

Дата: 13-05-20    Время: 17:16:00    Температура: 36°С

## 2. Режим контроля температуры:

The screenshot displays the ASFA-Intellect software interface for temperature control. The interface is divided into several sections:

- Top Panel:** Includes navigation tabs like 'Монитор', 'Поиск', 'База лиц', 'Распознавание файлов/папки', 'Аналитика', and 'Статистика'. It also features a 'Фильтры' section and a 'Создать заголовок панели' button.
- Table:** A table listing detected faces with columns for 'Зависимое лицо', 'Оригинал из БД', 'ФИО', 'Температура', 'Камера', and 'Дата'.

Зависимое лицо	Оригинал из БД	ФИО	Температура	Камера	Дата
		Гегамян Арутюн Арут' 83,7 %	38,2	Камера главный вход	13.05.2020 17:14:11
		Баларов Астерик Арут' 83,9 %	36,2	Камера главный вход	13.05.2020 17:14:06
		Говва Елизавета Арут' 56,3 %		Камера главный вход	13.05.2020 17:14:01
			35,9	Камера главный вход	13.05.2020 17:13:59
		Гоголева Юлия Арут' 54,8 %		Камера главный вход	13.05.2020 17:13:53
- Alerts:** A red banner at the top right reads 'Внимание! Гегамян Арутюн Температура: 38,2°'. A yellow banner at the bottom of the table reads 'Внимание! Высокая температура: 38.2 °C Дверь заблокирована'.
- Video Feed:** A large video window shows a person at a turnstile. A '94%' mask detection percentage is overlaid on the person's face. Below the video is a 'База лиц' and 'Камеры' section with a table of face images, names, similarity percentages, and dates.

Изображение	ФИО	Степень схожести	Комментарий	Дата
	Гегамян Арутюн Арут' 83,7 %	83,7 %		13.05.2020 14:19:05
- Bottom Panel:** A yellow banner displays 'ФИО: Гегамян Арутюн. (38.2°C)' and 'Аххон'. Below it, a status bar shows 'Дата: 13-05-20 Время: 17:14:12 Темп: 38.2°C' and a 'Выход' button.

On the right side of the image, there is a vertical strip showing a live video feed of a person in a white lab coat and mask standing at a turnstile. The video feed is labeled 'Монитор 4' and shows the timestamp '13-05-20 17:14:14'.

## 4 Работа программного модуля Виртуальный сервер доступа

Для работы с программным модулем *Виртуальный сервер доступа* наиболее часто используются следующие интерфейсные объекты:

1. **Протокол событий** (см. [Программный комплекс Интеллект: Руководство Администратора](#) и [Программный комплекс Интеллект: Руководство Оператора](#));
2. **Диспетчер событий** (см. [Руководство по настройке и работе с модулем Диспетчер событий](#));
3. **Бюро пропусков** (см. [Руководство по настройке и работе с модулем Бюро пропусков](#)).