Руководство по настройке и работе с модулем Виртуальный сервер доступа

ACFA Интеллект

Last update 01/17/2023

Table of Contents

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

На странице:

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 *ACFA-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 *ACFA-Интеллект* и служит для объединения работы программных комплексов *Auto-Интеллект* и *Face-Интеллект* с *ACFA-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.

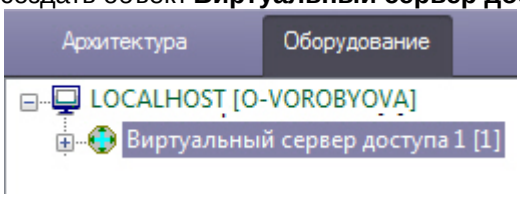
3 Настройка программного модуля Виртуальный сервер доступа

3.1 Настройка виртуальной точки прохода при распознавании номеров автомобилей

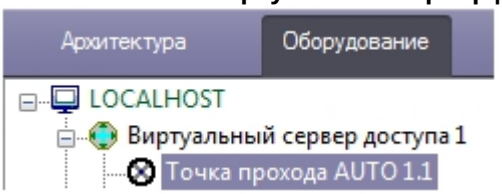
Организация виртуальной точки прохода при распознавании номеров автомобилей позволяет фиксировать проход (событие ACCESS_IN) при распознавании номера, который есть в базе данных (в параметрах пользователя, задаваемых в модуле *Бюро пропусков*).

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

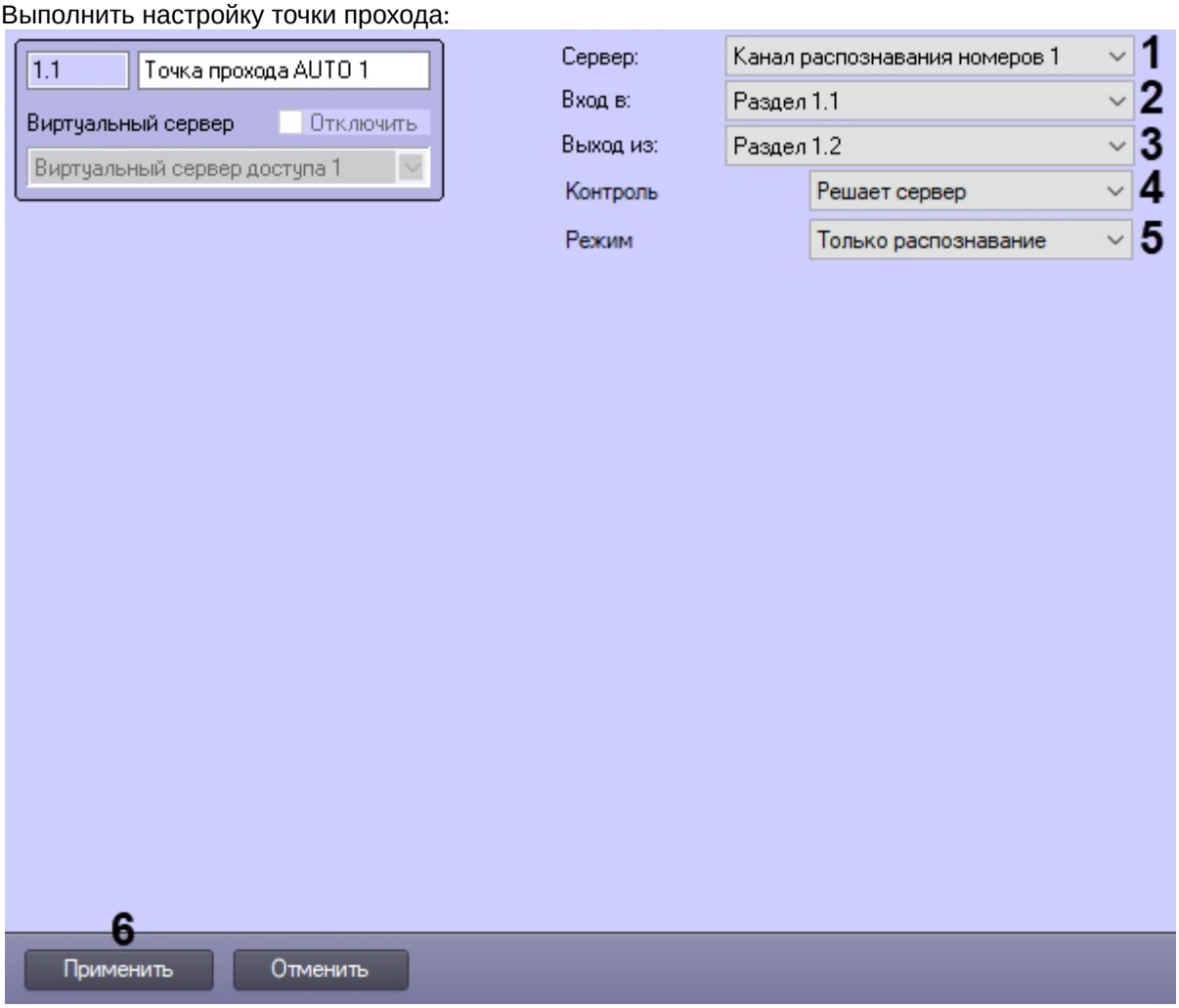
1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.



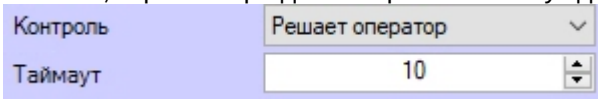
2. На базе объекта **Виртуальный сервер доступа** создать объект **Точка прохода AUTO**.



3. Выполнить настройку точки прохода:

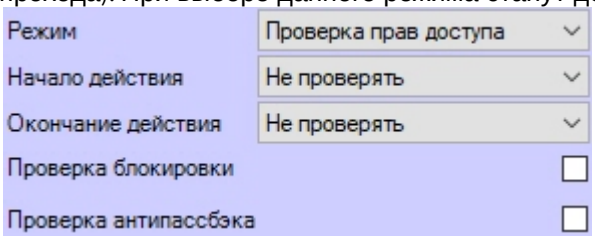


4. Выбрать канал распознавания номеров, на базе которого необходимо организовать точку прохода (**1**).
5. Из раскрывающегося списка **Вход в** выбрать объект **Раздел** соответствующий территории, в которую осуществляется вход (**2**).
6. Из раскрывающегося списка **Выход из** выбрать объект **Раздел** 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:



  - **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.

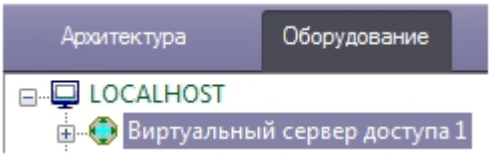
Организация виртуальной точки прохода при распознавании номеров автомобилей завершена.

3.2 Настройка виртуальной точки прохода при распознавании лиц

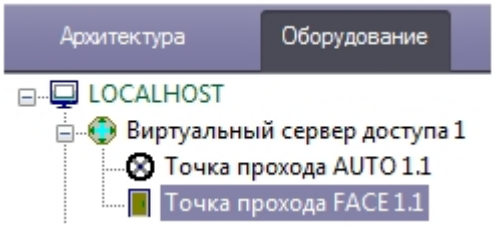
Организация виртуальной точки прохода при распознавании лиц позволяет фиксировать проход (событие ACCESS_IN) при распознавании лица, которое есть в базе данных (см. Программный комплекс Face-Интеллект. Руководство Администратора).

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**.



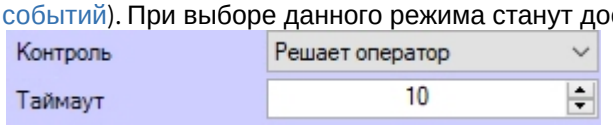
2. На базе объекта **Виртуальный сервер доступа** создать объект **Точка прохода FACE**.



3. Выполнить настройку точки прохода FACE:

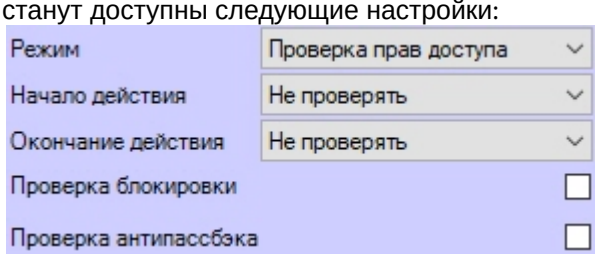
4. Выбрать камеру, которой осуществляется распознавание лиц. Камера должна работать в составе сервера распознавания лиц (**1**).
5. Выбрать сервер распознавания лиц, на базе которого необходимо организовать точку прохода (**2**).
6. Из раскрывающегося списка **Вход в** выбрать объект **Раздел** соответствующий 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:

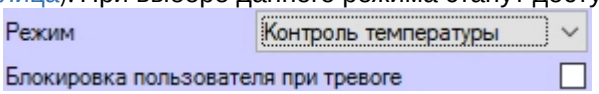


- **Таймаут** - задает в секундах временной интервал ожидания подтверждения доступа оператором. В течение заданного таймаута все прочие запросы от Сервера распознавания лиц игнорируются.

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:



     - **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:



     - **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.

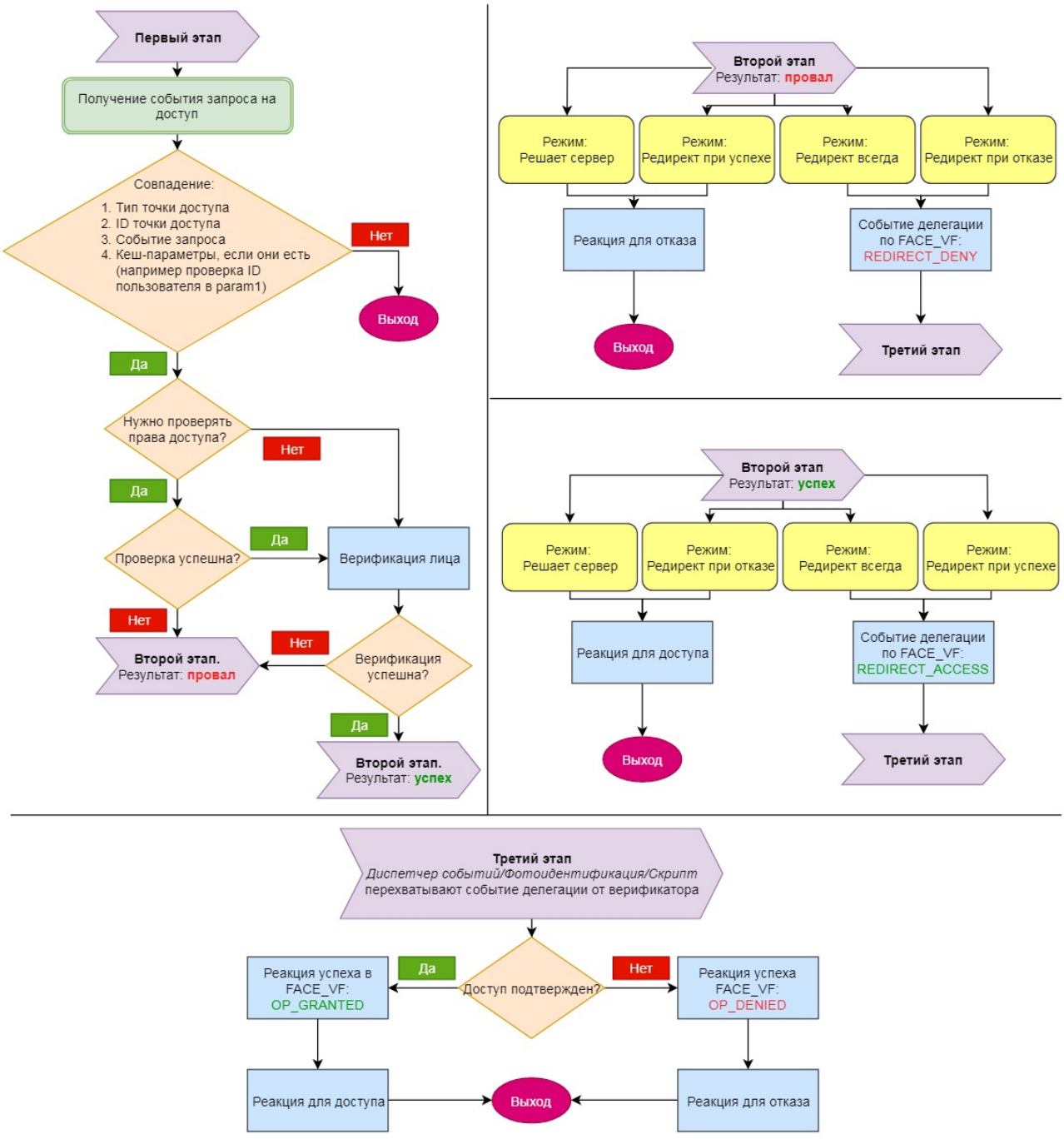
3.3 Организация двухфакторной верификации

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 происходить верификация лица.

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



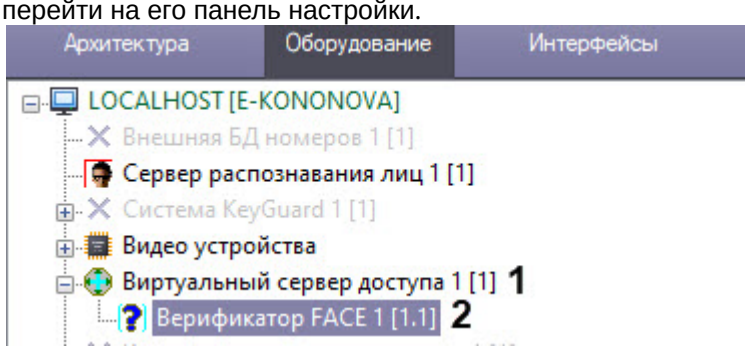
3.3.2 Настройка двухфакторной верификации

Организация двухфакторной авторизации включает в себя настройку на стороне ACFA и на стороне Face.

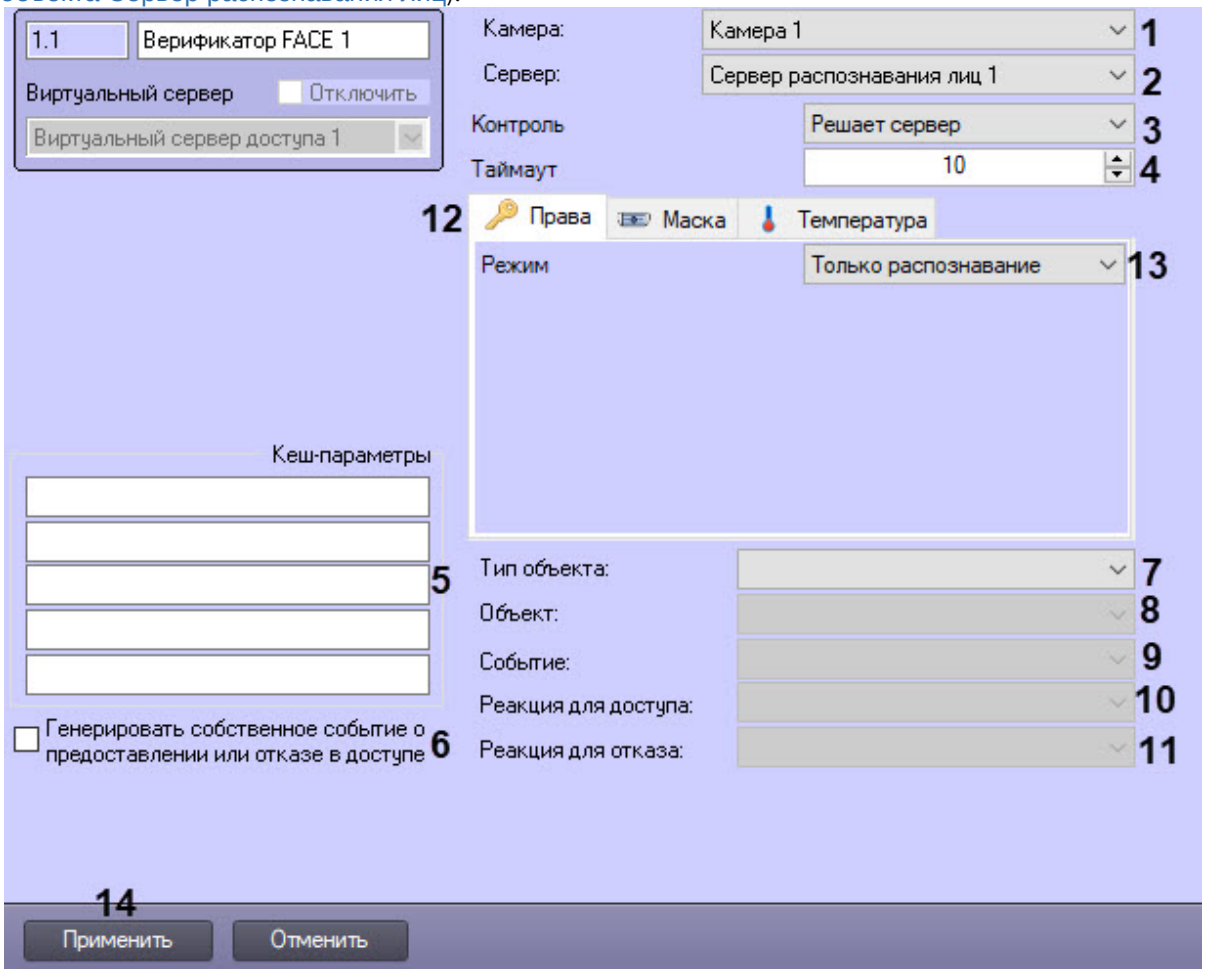
Настройка двухфакторной авторизации на стороне ACFA

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** (**1**).
2. На базе объекта **Виртуальный сервер доступа** создать объект **Верификатор FACE** (**2**) и перейти на его панель настройки.



3. Из раскрывающегося списка **Камера** (**1**) выбрать камеру, которая осуществляет захват лиц. Камера должна работать в составе **Сервера распознавания лиц** (см. Настройка системного объекта Сервер распознавания лиц).



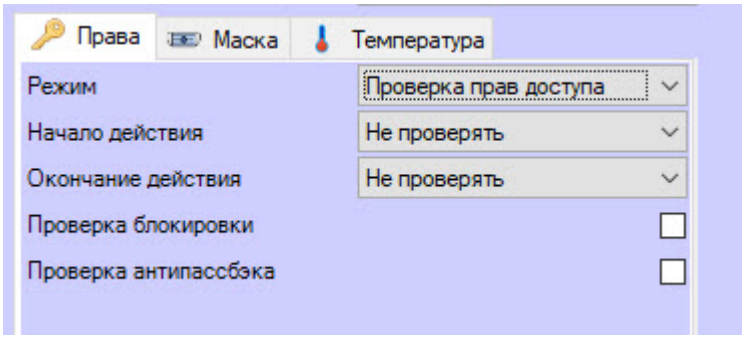
4. Из раскрывающегося списка **Сервер** (**2**) выбрать **Сервер распознавания лиц**.
5. Из раскрывающегося списка **Контроль** выбрать режим предоставления доступа (**3**):
   - **Решает сервер** – в зависимости от результата проверки прав доступа/верификации лица генерируется реакция для доступа или отказа.

- **Редирект всегда** – независимо от результата второго этапа верификатор перенаправляет своё решение на внешний верификатор (*Диспетчер событий/Фотоидентификацию/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.

6. Ввести значение поля **Таймаут** (**4**) – время в секундах, по истечении которого связь с **Сервером распознавания лиц** разрывается.
7. При необходимости в полях группы **Кеш-параметры** (**5**) задать параметры, индивидуальные для каждого программного модуля интеграции СКУД.

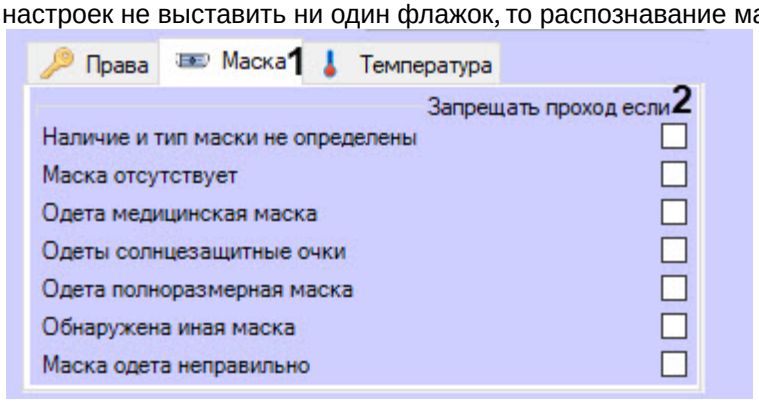
   > **Примечание**
   >
   > Например, в модуле интеграции *PERCo-S-20 v.2* каждый запрос оператору сопровождается параметром **request_id**. Этот параметр необходимо обязательно возвращать при подтверждении доступа, иначе команда будет проигнорирована. Для СКУД *Noder* таким параметром является **param1**.

8. Установить флажок **Генерировать собственное событие о предоставлении или отказе в доступе** (**6**), 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*.
9. Из раскрывающегося списка **Тип объекта** (**7**) выбрать тип объекта, который будет являться инициатором проверки лица. Как правило, это точка доступа, считыватель и т.п.
10. Из раскрывающегося списка **Объект** (**8**) выбрать объект заданного выше типа.
11. Из раскрывающегося списка **Событие** (**9**) выбрать событие, по которому будет запущена проверка лица. Список доступных событий зависит от выбранного типа объекта.
12. Из раскрывающегося списка **Реакция для доступа** (**10**) выбрать команду, которая будет отправлена на объект-инициатор при успешной верификации лица. Список доступных команд зависит от выбранного типа объекта.
13. Из раскрывающегося списка **Реакция для отказа** (**11**) выбрать команду, которая будет отправлена на объект-инициатор при неуспешной проверке/верификации лица. Список доступных команд зависит от выбранного типа объекта.
14. На вкладке **Права** (**12**) из раскрывающегося списка **Режим** выбрать режим проверки прав доступа (**13**):
    - **Только распознавание** – сервер принимает решение о предоставлении доступа только на основании верификации лица.
    - **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:

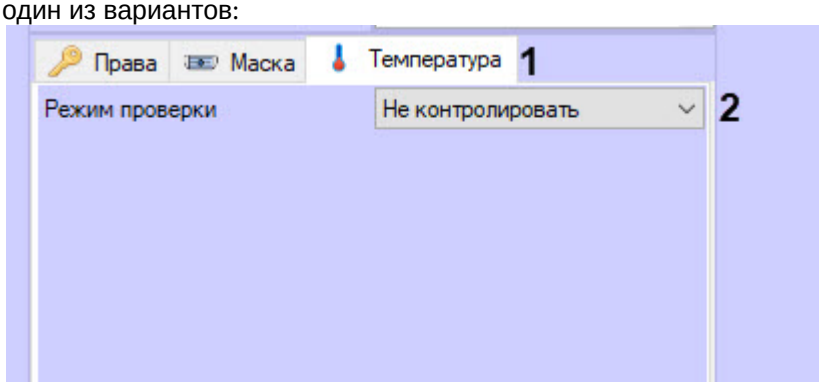


- **Начало действия** и **Окончание действия** – задает режим проверки срока действия карты доступа:
  - **Не проверять** – не проверять дату начала или окончания срока действия карты.
  - **Не включительно** – не включать в проверку дату начала или окончания срока действия карты.
  - **Включительно**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

15. Перейти на вкладку **Маска** (**1**) и установить флажки **Запрещать проход если** (**2**), чтобы высылался запрет доступа в зависимости от выставленных флажков. Если в данном блоке настроек не выставить ни один флажок, то распознавание маски будет игнорироваться.

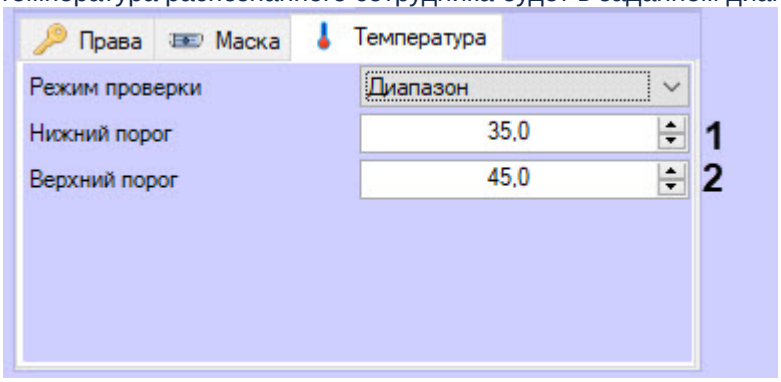


16. Перейти на вкладку **Температура** (**1**) и из выпадающего списка **Режим проверки** (**2**) выбрать один из вариантов:



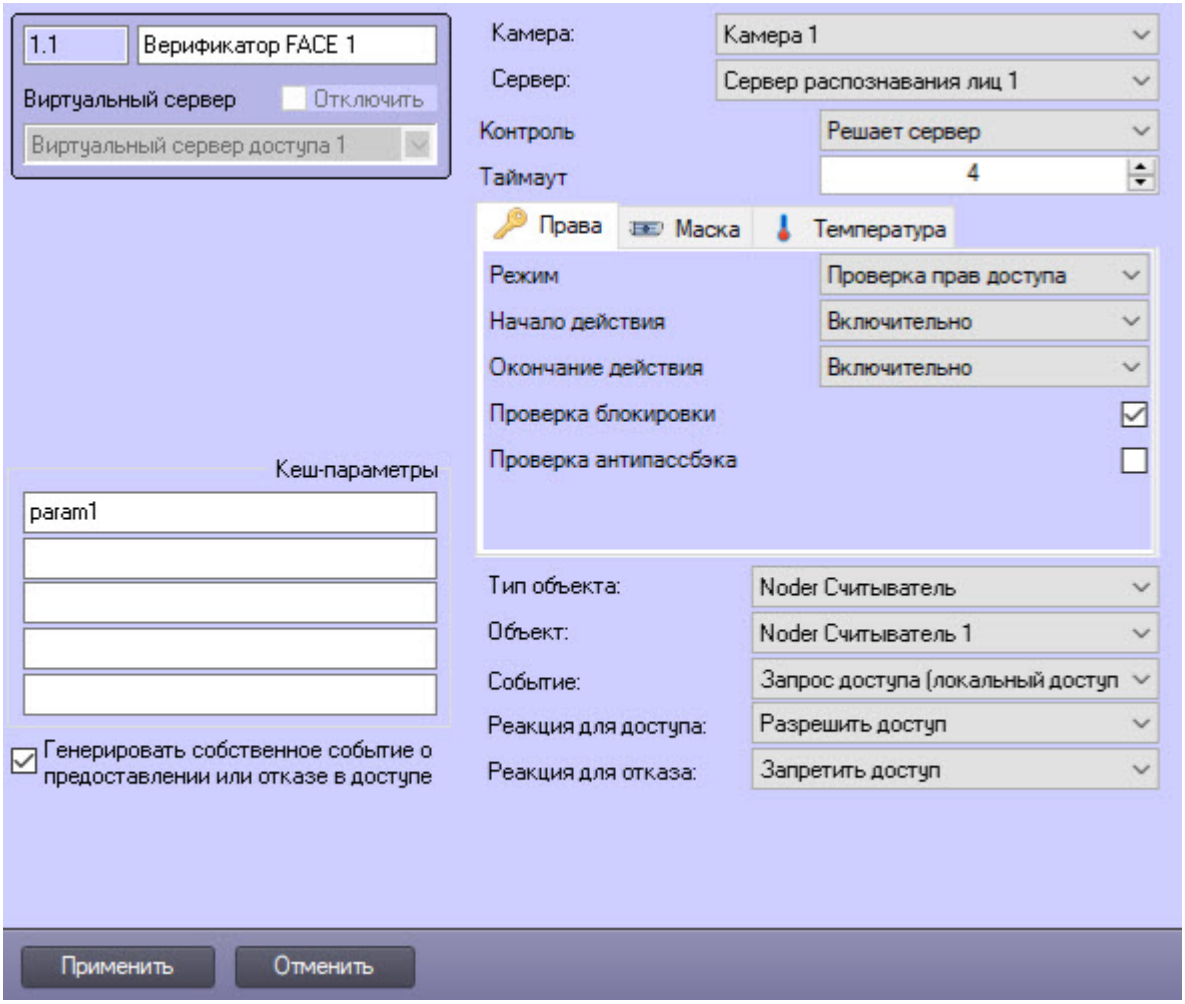
- **Не контролировать** – независимо от температуры у распознанного пользователя доступ будет разрешен.

- **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** (**1**) и **Верхний порог** (**2**) указать минимально и максимально допустимую температуру соответственно. Доступ разрешен, если температура распознанного сотрудника будет в заданном диапазоне.



17. Нажать кнопку **Применить** (**14**) для сохранения настроек.

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



Настройка двухфакторной верификации на стороне ACFA завершена.

Настройка двухфакторной авторизации на стороне Face

Для работы двухфакторной верификации не требуется база лиц.

На стороне Face 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 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, блокировать 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:
   a. 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**.

b. 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**:

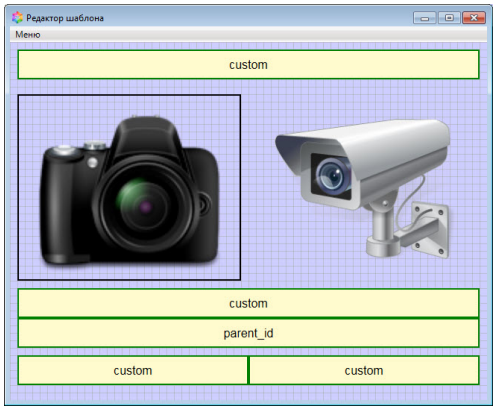
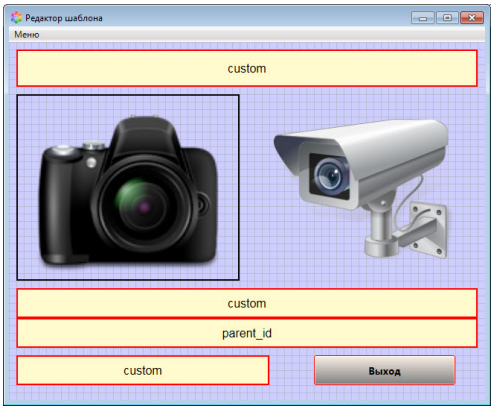
```
{date} {time}
```

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
	

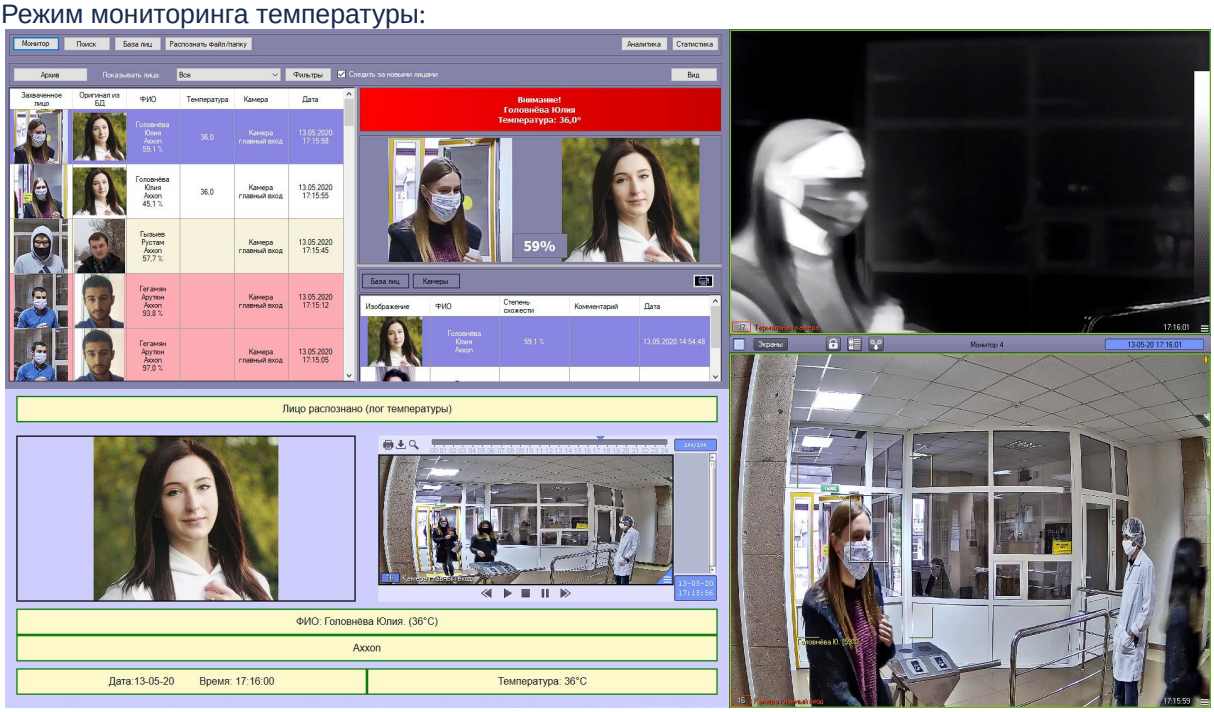
4. В случае необходимости отображения захваченного лица с камеры от Сервера распознавания лиц, когда лицо распознать не удалось, выполнить настройку программного модуля *Диспетчер событий* согласно документации. Обязательные настройки приведены ниже:
   a. Создать и настроить новый объект **Правило отображения**:
      - 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
```

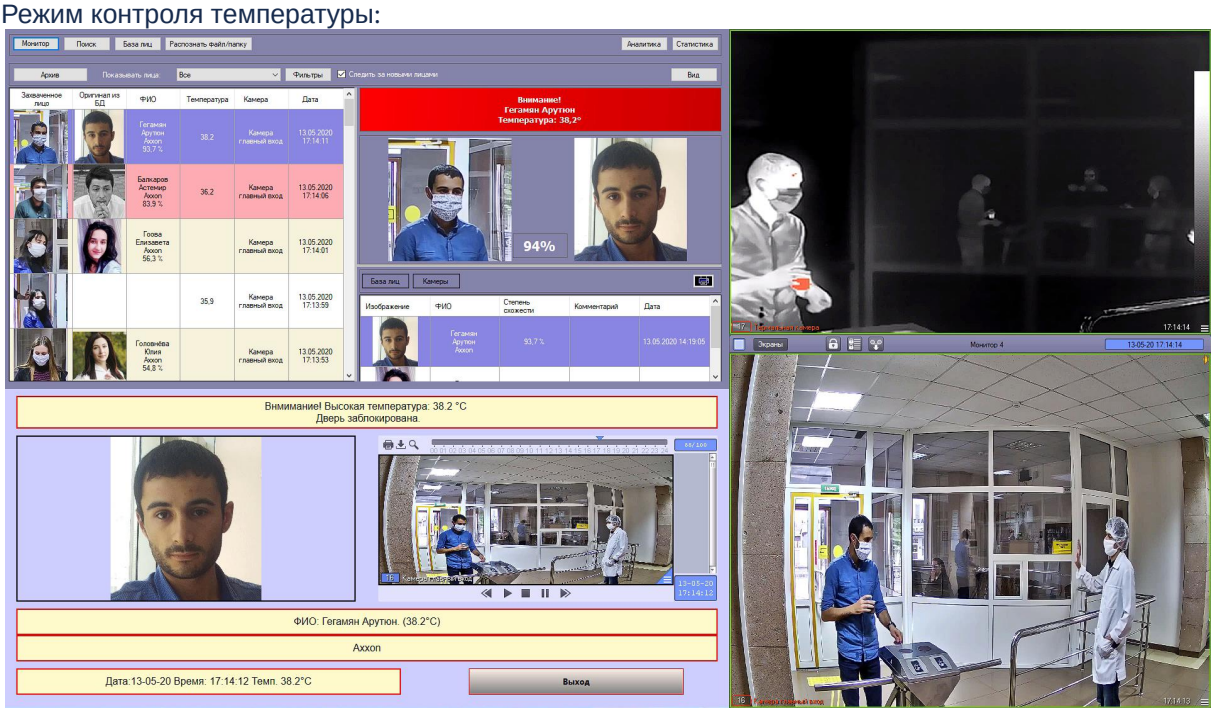
> Свойства объекта Фото пользователя

Пример настроенной системы мониторинга и контроля температуры лица:

1. Режим мониторинга температуры:



2. Режим контроля температуры:



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).