ACFA Intellect

Руководство по настройке и работе с модулем Виртуальный сервер доступа

Last update 18/03/2021

Содержание

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* доступа здесь.

2 Лицензирование модуля Виртуальный сервер доступа

Данный модуль не лицензируется.

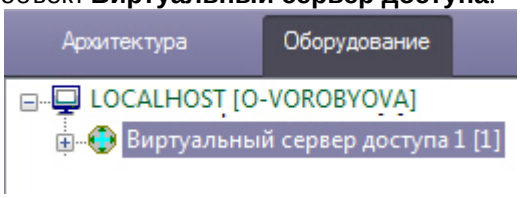
3 Настройка программного модуля Виртуальный сервер доступа

3.1 Настройка виртуальной точки прохода при распознавании номеров автомобилей

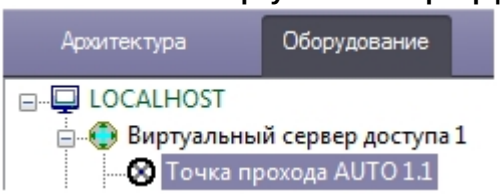
Организация виртуальной точки прохода при распознавании номеров автомобилей позволяет фиксировать проход (событие ACCESS_IN) при распознавании номера, который есть в базе данных (в настройках пользователя, задаваемых в программном модуле *Бюро пропусков*).

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

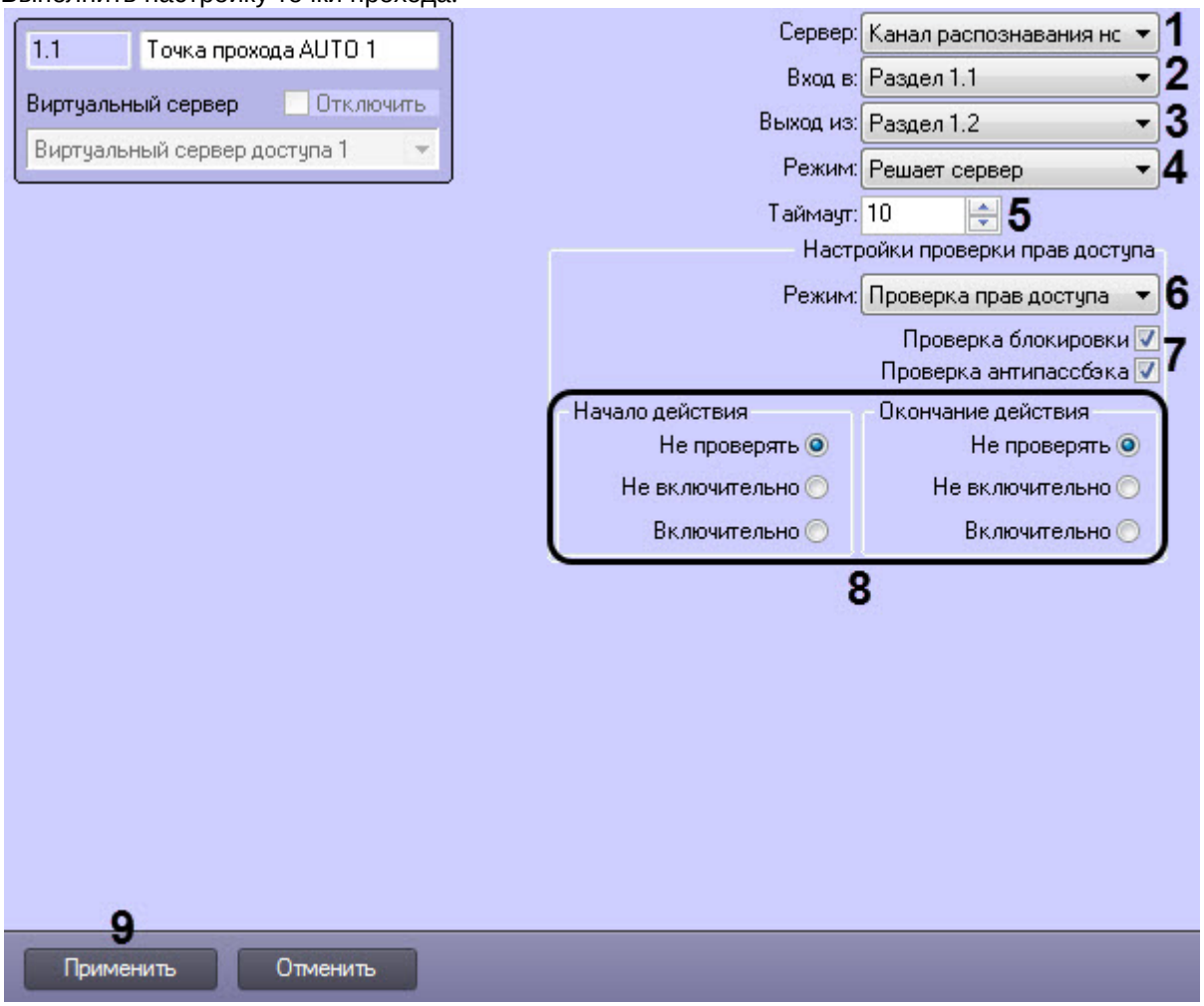
1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.



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



3. Выполнить настройку точки прохода:



   a. Выбрать сервер распознавания номеров, на базе которого необходимо организовать точку прохода (**1**).
   b. Из раскрывающегося списка **Вход в** выбрать объект **Раздел** соответствующий территории, в которую осуществляется вход (**2**).
   c. Из раскрывающегося списка **Выход из** выбрать объект **Раздел** соответствующий территории, из которой осуществляется выход (**3**).
   d. Из раскрывающегося списка **Режим** выбрать режим предоставления доступа: автоматически (в том числе при помощи скрипта, контролирующего датчики двери) или по подтверждению от оператора путем нажатия на кнопку в **Диспетчере событий** (см. Работа с программным модулем Диспетчер событий) (**4**).
   e. В поле **Таймаут** установить временной интервал ожидания подтверждения доступа в секундах (**5**).

      Примечание

      В течение выбранного таймаута все прочие запросы от сервера распознавания номеров игнорируются.

   f. Настроить режим проверки прав доступа (**6**):
      - Если необходимо принимать решение о предоставлении доступа только на основании распознавания номеров установить режим **Только распознавание**.
      - Если необходимо осуществлять проверку уровня доступа пользователя, которому принадлежит автомобиль, и временных зон этого уровня доступа, а также выполнять дополнительные проверки, выбрать режим **Проверка прав доступа** и установить флажки напротив тех проверок, которые необходимо осуществлять (**7**).

1. **Проверка блокировки** – если пользователь заблокирован, доступ предоставлен не будет.
2. **Проверка антипассбэка** – контроль двойного прохода через точку доступа.

> **Примечание.**
>
> Проверка уровня доступа и его временных зон будет осуществляться при режиме **Проверка прав доступа** всегда.

g. В разделе **Начало действия** и **Окончание действия** установить переключатель в положение, соответствующее настройке проверки срока действия карты, указанного в интерфейсном модуле *Бюро пропусков* (**8**).
   - **Не проверять** – если проверка срока действия карты не требуется.
   - **Не включительно** – не включать в проверку дату истечения срока действия карты.
   - **Включительно** – включать в проверку дату истечения срока действия карты.

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

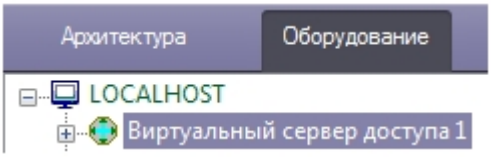
Организация виртуальной точки прохода при распознавании номеров автомобилей завершена.

3.2 Настройка виртуальной точки прохода при распознавании лиц

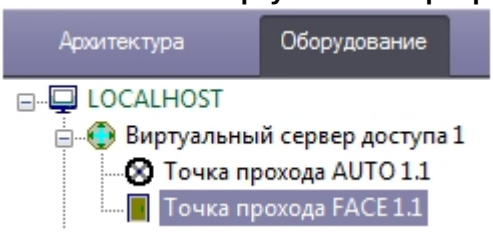
Организация виртуальной точки прохода при распознавании лиц позволяет фиксировать проход (событие ACCESS_IN) при распознавании лица, которое есть в базе данных (см. Программный комплекс Face-Интеллект. Руководство администратора).

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

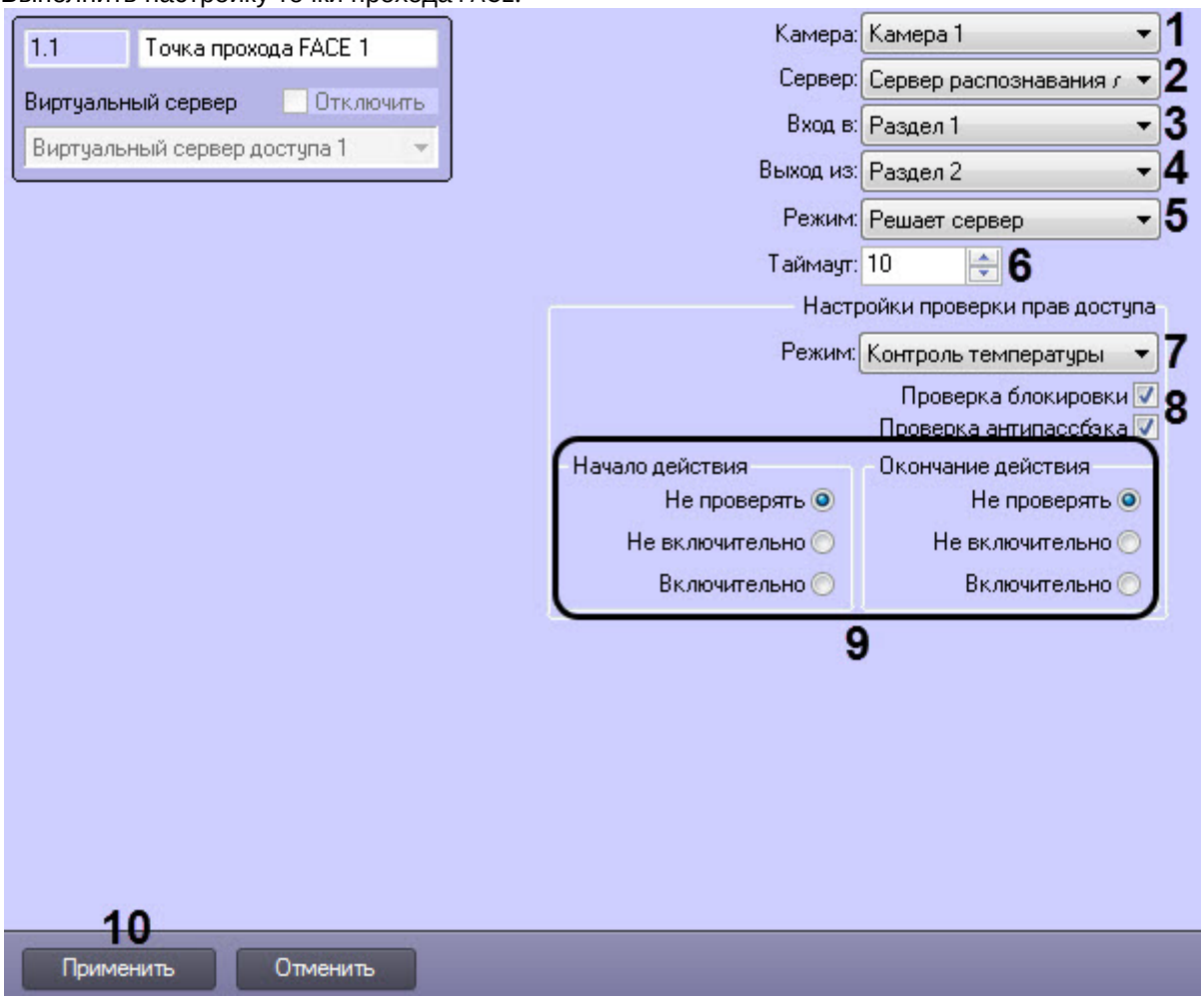
1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.



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



3. Выполнить настройку точки прохода FACE:



a. Выбрать камеру, которой осуществляется распознавание лиц. Камера должна работать в составе сервера распознавания лиц (**1**).
b. Выбрать сервер распознавания лиц, на базе которого необходимо организовать точку прохода (**2**).
c. Из раскрывающегося списка **Вход в** выбрать объект **Раздел** соответствующий территории, в которую осуществляется вход (**3**).
d. Из раскрывающегося списка **Выход из** выбрать объект **Раздел** соответствующий территории, из которой осуществляется выход (**4**).
e. Из раскрывающегося списка **Режим** выбрать режим предоставления доступа: автоматически (в том числе при помощи скрипта, контролирующего датчики двери) или по подтверждению от оператора путем нажатия на кнопку в **Диспетчере событий** (см. Работа с программным модулем Диспетчер событий) (**5**).
f. В поле **Таймаут** установить временной интервал ожидания подтверждения доступа в секундах (**6**).

> **Примечание**
>
> В течение выбранного таймаута все прочие запросы от сервера распознавания лиц игнорируются.

g. Настроить режим проверки прав доступа (**7**):
   - Если необходимо принимать решение о предоставлении доступа только на основании распознавания лиц, установить режим **Только распознавание**.
   - Если необходимо осуществлять проверку уровня доступа пользователя, чье лицо оказалось распознано, и временных зон этого уровня доступа, а также выполнять дополнительные

проверки, выбрать режим **Проверка прав доступа** и установить флажки напротив тех проверок, которые необходимо осуществлять (**8**).

1. **Проверка блокировки** – если пользователь заблокирован, доступ предоставлен не будет.
2. **Проверка антипассбэка** – контроль двойного прохода через точку доступа.

> **Примечание.**
>
> Проверка уровня доступа и его временных зон будет осуществляться при режиме **Проверка прав доступа** всегда.

- **Мониторинг температуры** - если требуется осуществлять только мониторинг температуры лица (см. Организация мониторинга и контроля температуры лица).
- **Контроль температуры** - если требуется осуществлять контроль превышения порога температуры лица (см. Организация мониторинга и контроля температуры лица).

h. В разделе **Начало действия** и **Окончание действия** установить переключатель в положение, соответствующее настройке проверки срока действия карты, указанного в интерфейсном модуле *Бюро пропусков* (**9**).
   - **Не проверять** – если проверка срока действия карты не требуется.
   - **Не включительно** – не включать в проверку дату истечения срока действия карты.
   - **Включительно** – включать в проверку дату истечения срока действия карты.

4. Нажать кнопку **Применить** (**10**) для сохранения изменений.

Организация виртуальной точки прохода при распознавании лиц завершена.

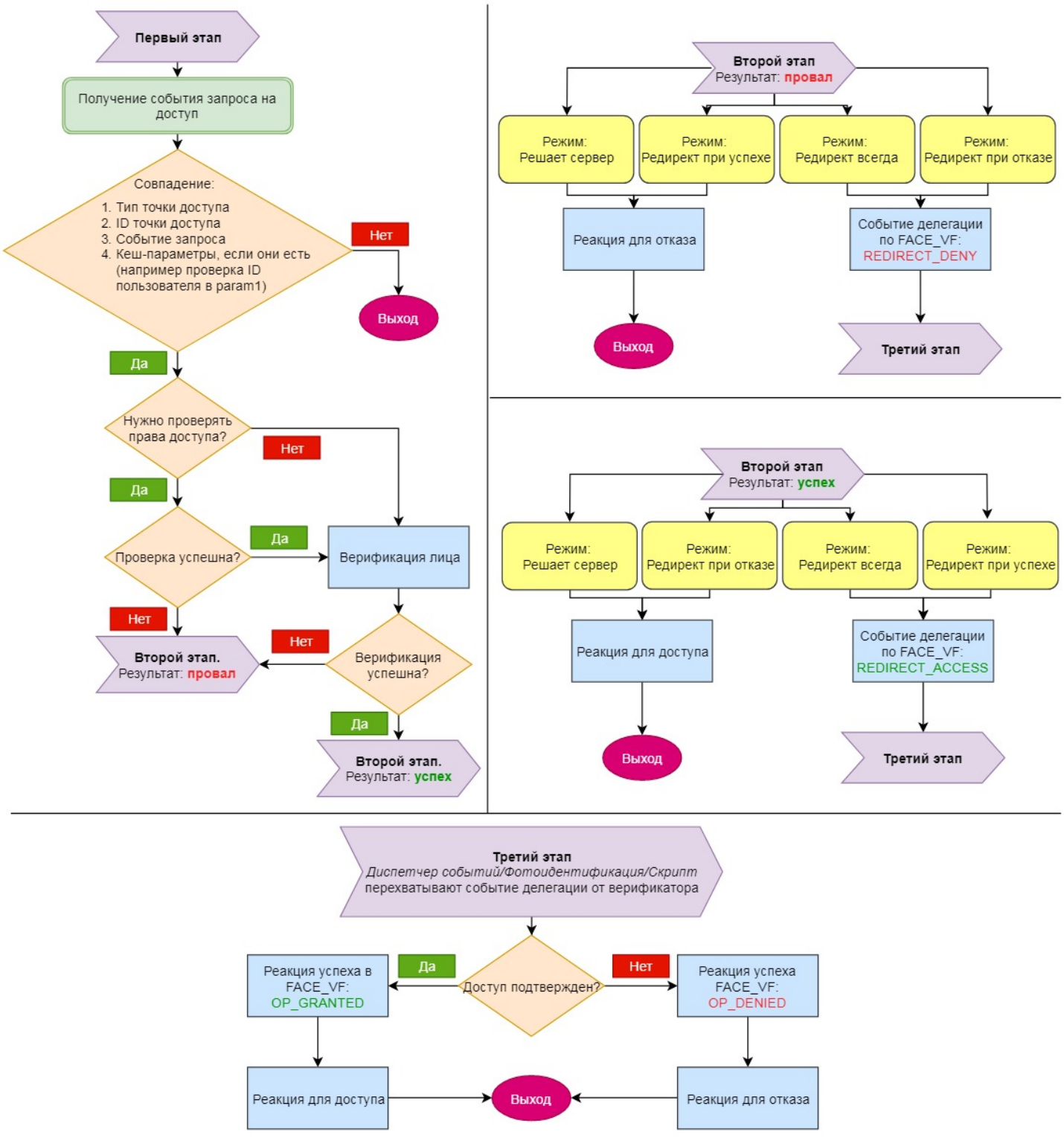
3.3 Организация двухфакторной верификации

3.3.1 Общие сведения о двухфакторной верификации

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

> **Внимание!**
>
> В данном режиме первой всегда должна прикладываться карта доступа пользователя и только затем происходить верификация лица.

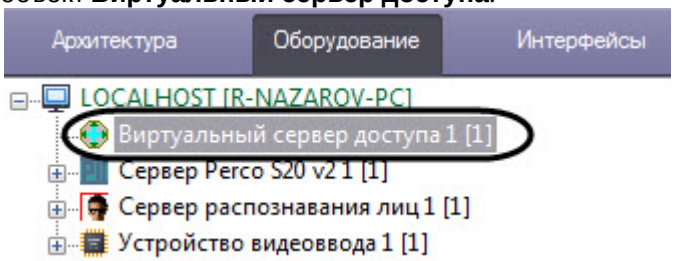
Двухфакторная верификация происходит в несколько этапов. Блок схема работы двухфакторной верификации представлена ниже.



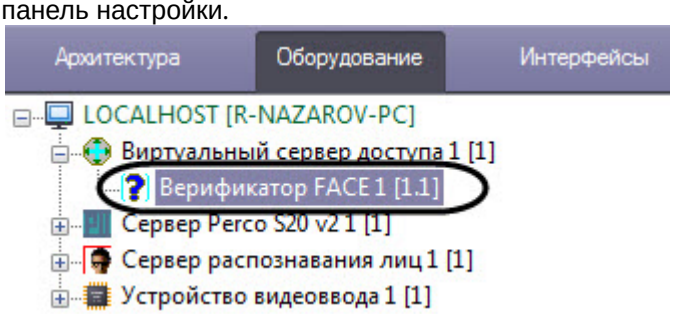
3.3.2 Настройка двухфакторной верификации

Для настройки двухфакторной верификации необходимо выполнить следующие действия:

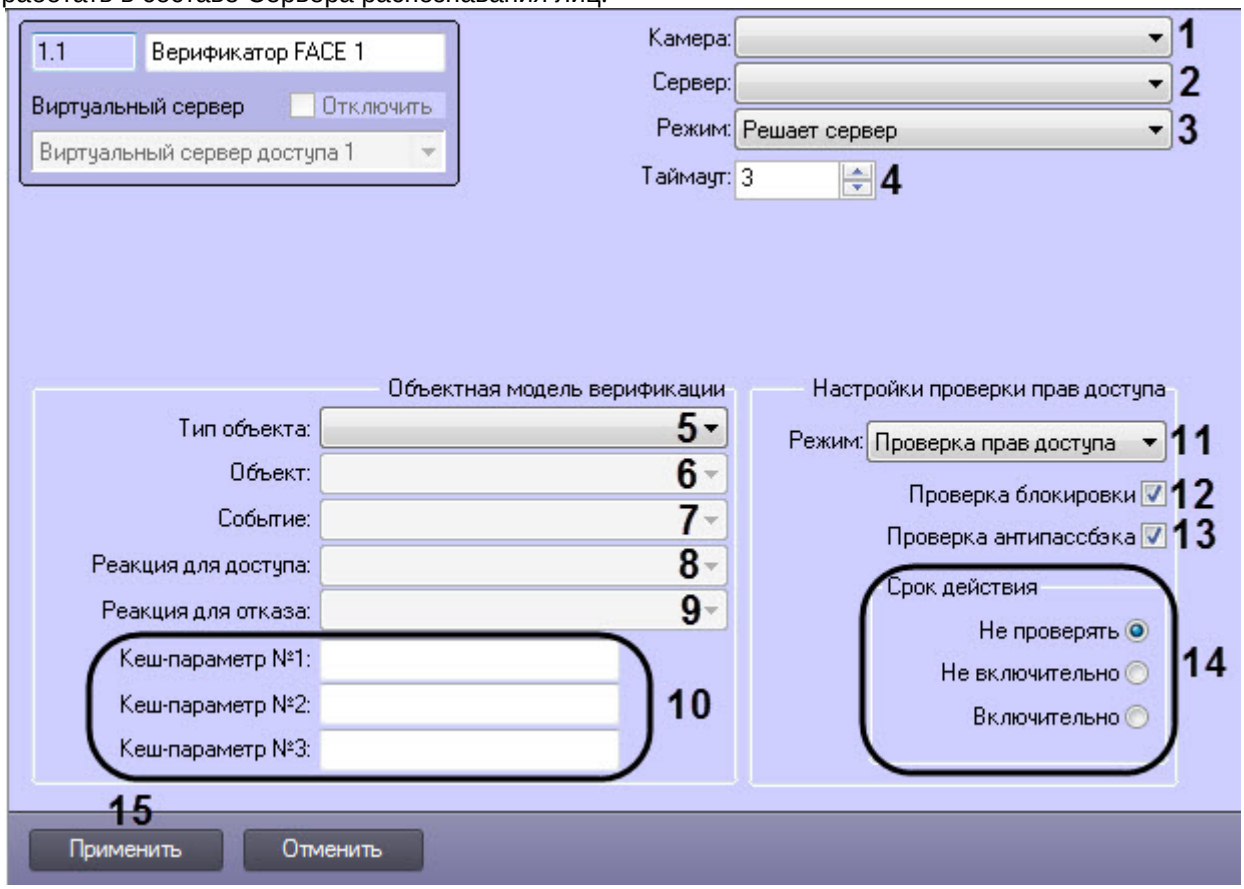
1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.



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



4. Из раскрывающегося списка **Сервер** (**2**) выбрать Сервер распознавания лиц.
5. Из раскрывающегося списка **Режим** (**3**) выбрать режим работы верификатора:
   - **Решает сервер** - в зависимости от результата проверки/верификации лица генерируется реакция для доступа или отказа.
   - **Редирект всегда** - вне зависимости от результата второго этапа верификатор перенаправляет своё решение на *Диспетчер событий/Фотоидентификацию/Скрипт* с помощью события делегации и

ожидает решение внешнего верификатора. 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.

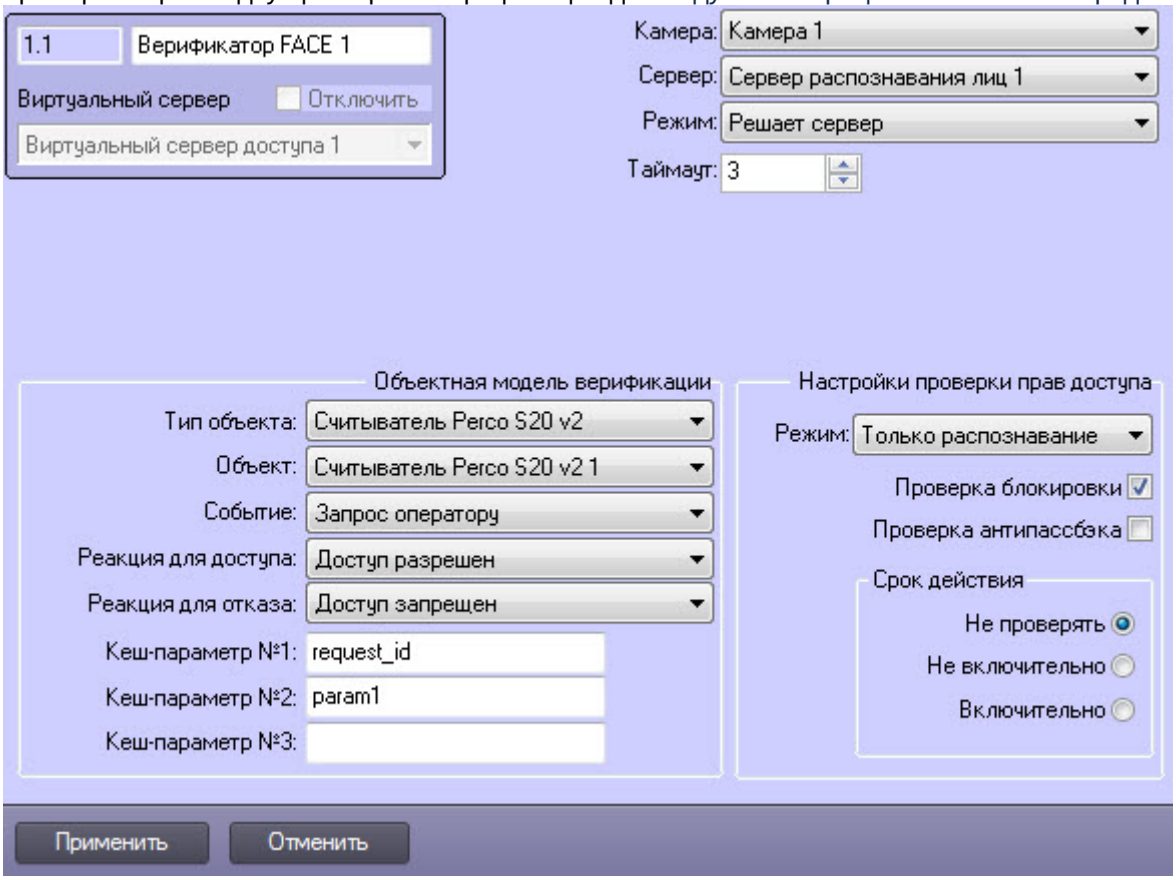
6. В поле **Таймаут** (**4**) задать время ожидания лица в камере Сервера распознавания лиц. Если лицо не появится перед камерой в течение данного времени, то верификация лица будет провалена.
7. Из раскрывающегося списка **Тип объекта** (**5**) выбрать тип объекта, который будет являться инициатором проверки лица. Как правило это точка доступа, считыватель и т.п.
8. Из раскрывающегося списка **Объект** (**6**) выбрать объект заданного выше типа.
9. Из раскрывающегося списка **Событие** (**7**) выбрать событие, по которому будет запущена проверка лица. Список доступных событий зависит от выбранного типа объекта.
10. Из раскрывающегося списка **Реакция для доступа** (**8**) выбрать команду, которая будет отправлена на объект-инициатор при успешной верификации лица. Список доступных команд зависит от выбранного типа объекта.
11. Из раскрывающегося списка **Реакция для отказа** (**9**) выбрать команду, которая будет отправлена на объект-инициатор при неуспешной проверке/верификации лица. Список доступных команд зависит от выбранного типа объекта.
12. При необходимости в полях **Кеш-параметры №1-N3** (**10**) задать параметры, которые индивидуальны для каждого программного модуля интеграции СКУД, с которым осуществляется работа.

> **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**.

13. Из раскрывающегося списка **Режим** (**11**) выбрать режим проверки прав доступа:
    a. **Проверка прав доступа** - активирует проверку прав доступа пользователя по параметрам ниже. Только после проверки прав доступа, в случае успеха, будет осуществяться верификация по лицу.
    b. **Только распознавание** - пропускает проверку прав доступаи переходит сразу к верификации лица.
14. Установить флажок **Проверка блокировки** (**12**), если необходимо проверять заблокирован ли пользователь или нет.
15. Установить флажок **Проверка антипассбэка** (**13**), если необходимо осуществлять проверку контроля двойного прохода.
16. Выбрать способ проверки срока действия карты доступа пользователя (**14**):
    - **Не проверять** - проверка срока действия карты осуществляться не будет.
    - **Не включительно** - в день истечения срока действия карты пользователю будет отказано в доступе.
    - **Включительно** - в день истечения срока действия карты пользователю доступ будет разрешен.
17. Нажать кнопку **Применить** (**15**) для сохранения настроек.

> **Внимание!**
>
> Параметры с (**1**) по (**9**) являются обязательными. Если не указать хотя бы один из них, то все выбранные значения данных параметров будут сброшены по умолчанию даже после нажатия кнопки **Применить**.

Пример настройки двухфакторной верификации для модуля интеграции *PERCo-S-20 v.2* представлен ниже.



Настройка двухфакторной верификации 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**:

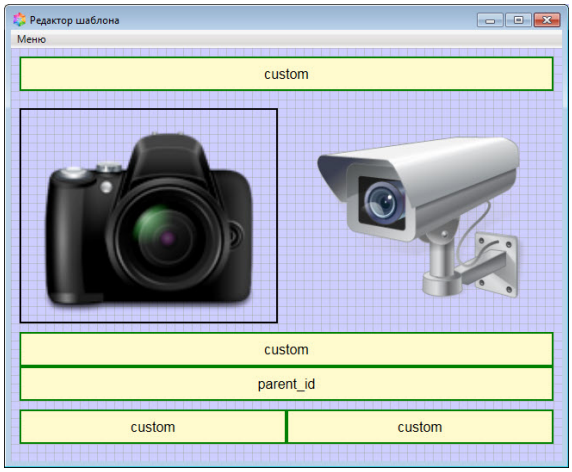
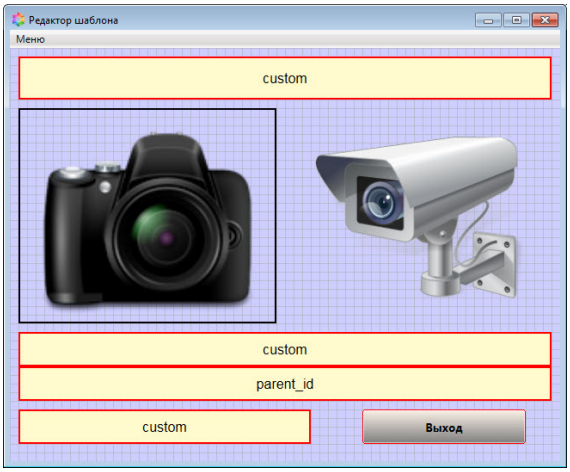
      ```
      {temperature}
      ```

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
	

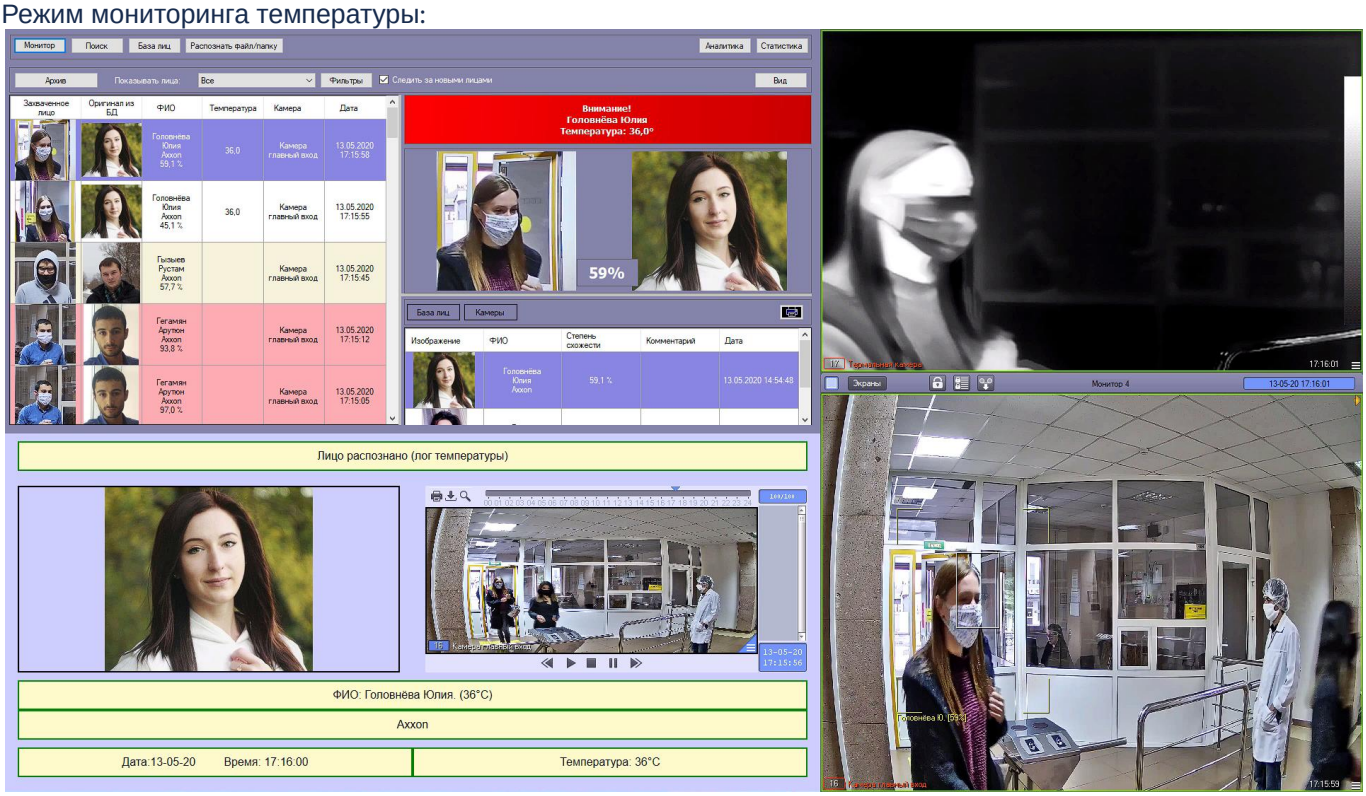
4. В случае необходимости отображения захваченного лица с камеры от Сервера распознавания лиц, когда лицо распознать не удалось, выполнить настройку программного модуля *Диспетчер событий* согласно документации. Обязательные настройки приведены ниже:
   a. Создать и настроить новый объект **Правило отображения**: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

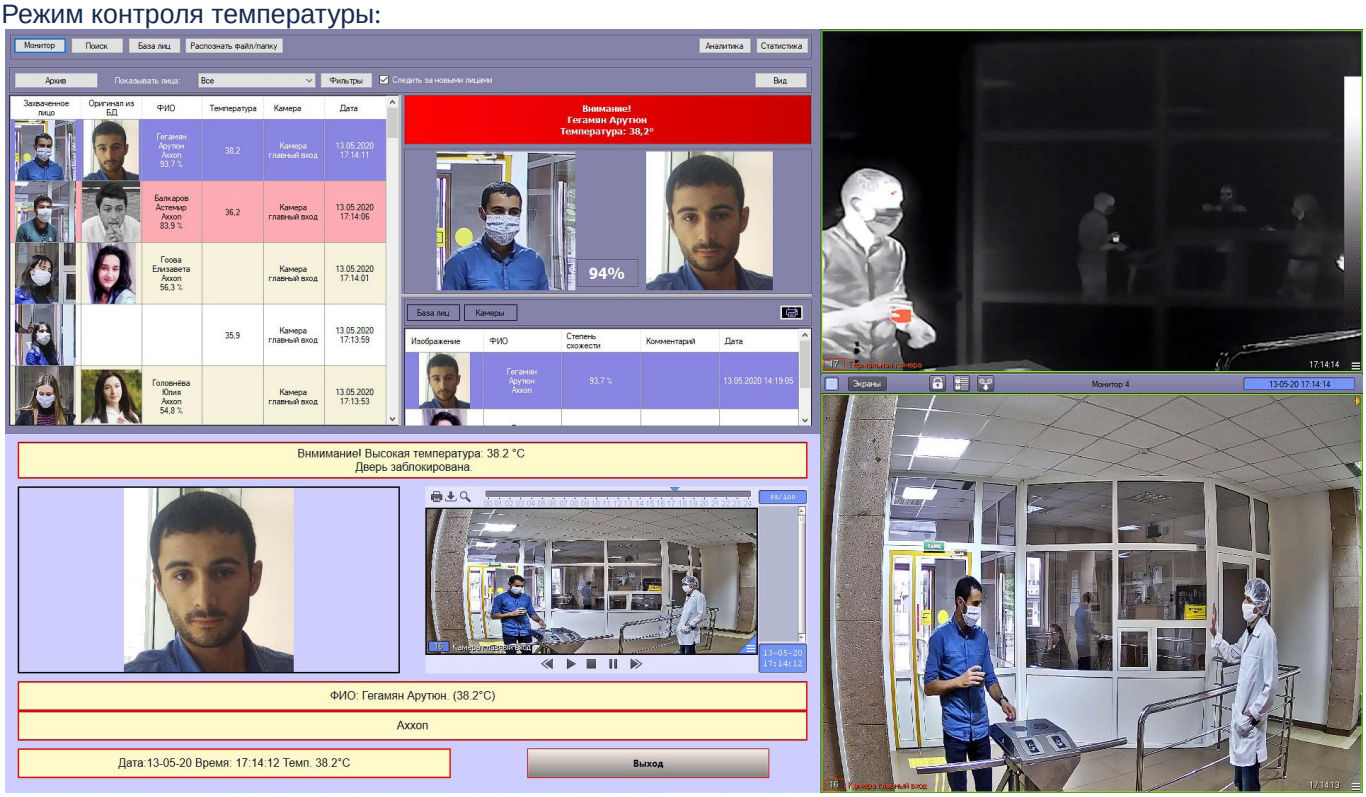
Свойства объекта Фото пользователя

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).