Руководство
по интеграции Domination Analytics Service со СКУД Sigur

1. Лицензионное соглашение

Настоящее Лицензионное соглашение является документом, регулирующим правила использования программного продукта Domination (далее «Программа») лицом, обладающим правомерно изготовленным и введенным в гражданский оборот экземпляром данного продукта («Лицензиатом»).

Настоящее Лицензионное соглашение действует в течение всего срока эксплуатации Лицензиатом Программы и/или нахождения у него экземпляров Программы. Устанавливая Программу, осуществляя ее запись в память ЭВМ, Лицензиат признает правила настоящего Лицензионного соглашения.

По настоящему Лицензионному соглашению Лицензиат получает право использовать Программу способами, описанными ниже.

АВТОРСКИЕ ПРАВА

Программа защищена национальными законами и международными соглашениями об авторском праве. Все исключительные авторские права на Программу принадлежат правообладателю. При распространении программы обязательно указывается имя правообладателя, его контактная информация и сайт правообладателя.

ПРАВА УСТАНОВКИ И ИСПОЛЬЗОВАНИЯ

Лицензиат имеет право устанавливать и использовать Программу на компьютерах:

– при приобретении Программы в комплекте с видеосервером на материальном носителе на неограниченном количестве компьютеров;

– при приобретении Программы через Интернет на неограниченном количестве компьютеров.

После установки Программы Лицензиат получает право использовать Программу и ее компоненты бесплатно, без лицензионных отчислений неограниченное время согласно условиям данного Лицензионного соглашения.

Программа поставляется «как есть».

Лицензиат обязуется не допускать нарушений исключительных прав правообладателя на Программу, в частности, не совершать и не допускать совершения следующих действий без специального письменного разрешения правообладателя:

1) распространять части программы, ее компоненты отдельно от остальных компонентов программы;

2) запрещено коммерческое распространение Программы (за распространение Программы запрещено брать деньги);

3) вносить какие-либо изменения в код Программы, за исключением тех, которые вносятся штатными средствами, входящими в состав Программы и описанными в сопроводительной документации;

4) осуществлять доступ к информационной базе Программы и построение систем на основе Программы с помощью средств и технологических решений, не предусмотренных в сопроводительной документации;

5) совершать действия, результатом которых является устранение или снижение эффективности технических средств защиты авторских прав, применяемых правообладателем Программы, включая применение программных и технических средств «мультиплексирования», средств, изменяющих алгоритм работы программных или аппаратных средств защиты Программы, а также использовать Программу с устраненными или измененными без разрешения Правообладателя средствами защиты;

6) восстанавливать исходный код, декомпилировать и/или деассемблировать программную часть системы, менять что-либо в ней и дополнять ее новыми функциями, за исключением тех случаев, и лишь в той степени, в какой такие действия специально разрешены действующим законодательством.

Программа может включаться в состав платных сборников, помещаться на сайтах, отличных от сайта правообладателя только с разрешения правообладателя.

ОГРАНИЧЕНИЕ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ

Программа может содержать ошибки. Правообладатель не несет ответственности за возможные ошибки Программы.

Правообладатель не гарантирует, что функции, содержащиеся в Программе, будут удовлетворять заявленным требованиям, или что работа Программы не прервется из-за ошибки.

Правообладатель намеренно отказывается от всех письменно заявленных и предполагаемых по умолчанию гарантийных обязательств, включая ограничения в применении гарантийных обязательств после определенного срока и годности Программы к продаже.

Ни при каких обстоятельствах правообладатель не несет обязательств перед пользователем за любой вред, физический или коммерческий, нанесенный данной Программой, включая упущенную прибыль, потерю данных, ущерб репутации или другой побочный, или косвенный вред, произошедший из-за использования или неспособности использования данной Программы. Также не принимаются иски на любые другие имущественные требования пользователя Программы.

КОНТРОЛЬ НАД СОБЛЮДЕНИЕМ ОБЯЗАТЕЛЬСТВ

Это Лицензионное соглашение соответствует национальным законам об авторском праве. Данное Лицензионное соглашение основано на новой редакции этих законов, что отменяет все остальные договоренности и соглашения, ранее применяемые по отношению к данной Программе.

Все спорные вопросы решаются по взаимной договоренности сторон, а если соглашения не было достигнуто, то в судебном порядке в порядке, предусмотренном действующим законодательством Российской Федерации.

Контактная информация

ООО «ВИПАКС+»
Юридический адрес: 115162, г. Москва, вн. тер. г. муниципальный округ Якиманка, ул. Мытная, д. 40, к. 4, кв. 135
Фактический адрес: 614015, г. Пермь, ул. Краснова, д. 24
Почтовый адрес: 614015, г. Пермь, а/я 1662
Тел. 8-800-101-01-32
E-mail: info@vipaks.com
Сайт: https://vipaks.com/

2. Интеграция со СКУД Sigur

Описание.

Двухфакторная верификация с помощью модуля «Распознавание лиц» Domination.

Данный сценарий может применяться, например, на проходной предприятия. Дополнительно к считывателю карт доступа устанавливается камера, направленная на проходящих через турникет людей. Система сравнивает лицо сотрудника с его фотографией в БД СКУД. Проход разрешен, если карта и лицо проходящего совпадают с шаблоном.

Функция работает в двух режимах:

- запрет доступа, если лицо не распознано;
- предоставление доступа, но с отметкой о нераспознанном лице в интерфейсе наблюдения

Режимы доступа:

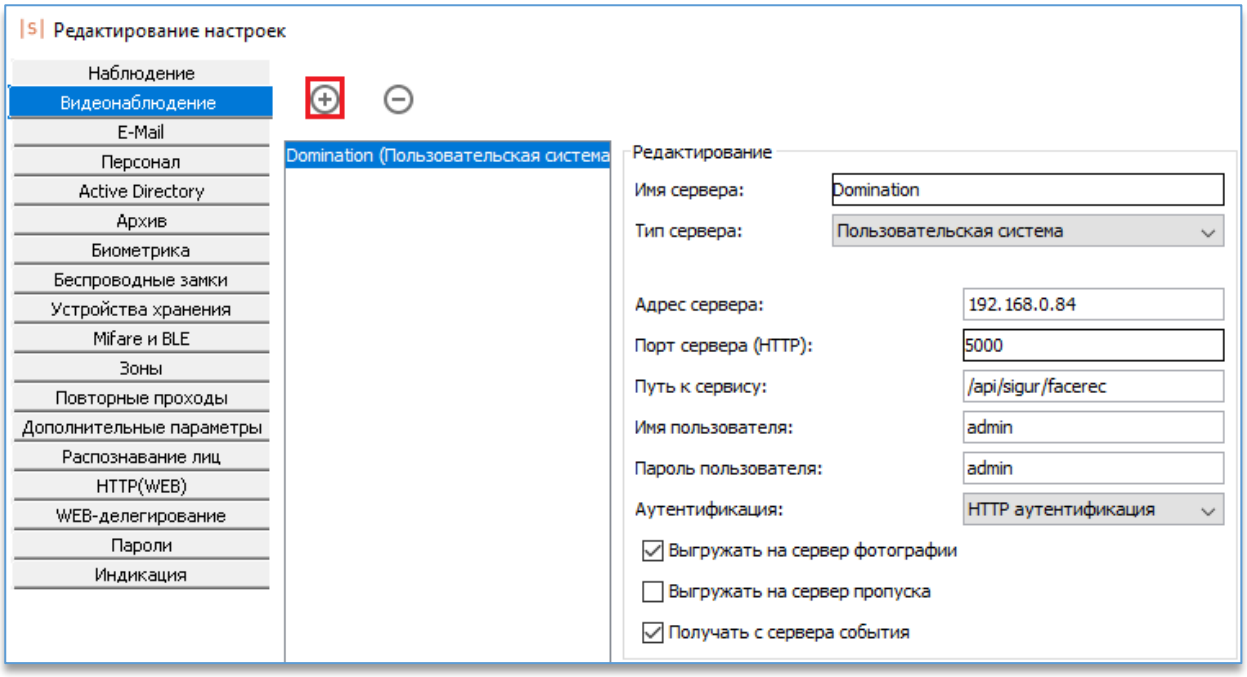
- «Только лицо».
  В данном случае распознанное лицо сотрудника является единственным признаком, на основе которого система принимает решение о предоставлении доступа. Это наиболее удобный режим работы, поскольку не требует от персонала никаких действий.
- «Карта или лицо».
  В данном случае распознанное лицо выступает в качестве дополнительного признака, на основе которого система принимает решение о предоставлении доступа. Основным может быть любой другой идентификатор (например, карта). Система предоставляет доступ в любом случае, однако если лицо так и не было распознано, будет выведено соответствующее событие в интерфейсе наблюдения.
- «Карта и лицо» (двойная идентификация);
  После идентификации по основному признаку (карта, пропуск) система производит сравнение изображения, полученного с камеры, с фотографией сотрудника. В случае если лицо не распознано или сотрудник не появился в кадре в течение 5 сек., система запрещает доступ.

Настройка.

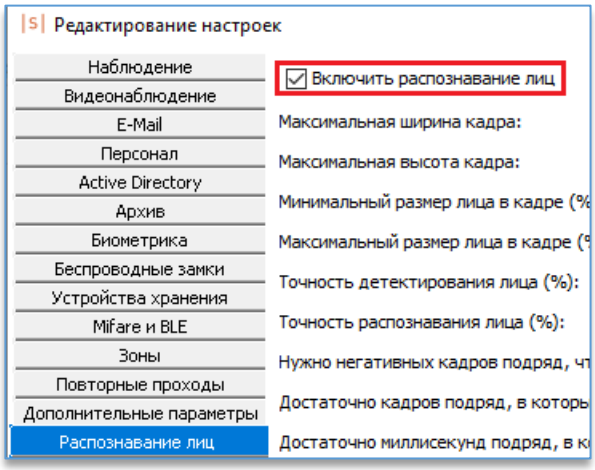
В программе управления Sigur необходимо зайти в «**Файл – Настройки**», далее в меню «**Видеонаблюдение**». Для добавления сервера аналитики Domination необходимо нажать на кнопку добавления, слева в окне указать данные для сервера:

- «**Имя сервера**». Любое название для сервера;
- «**Тип сервера**. Необходимо выбрать «**Пользовательская система**»;
- «**Адреса сервера**». Необходимо указать адрес ПК, на котором установлен сервер аналитики;
- «**Порт сервера (HTTP)**». Необходимо указать порт сервера аналитики (по умолчанию 5000);
- «**Путь к сервису**». В данной строке требуется прописать «*/api/sigur/facerec*»;
- «**Имя пользователя**». Имя (логин) от сервера аналитики. Рекомендуется указывать пользователя admin либо другого, который находится в группе «**Администраторы**» в сервере аналитики;
- «**Пароль**». Пароль от пользователя сервера аналитики;
- «**Аутентификация**». Необходимо указать «**HTTP аутентификация**».

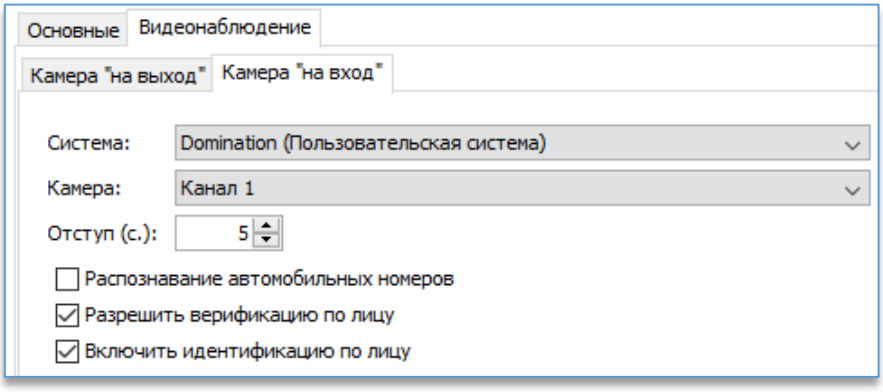
Ниже для выгрузки персон из базы Sigur в базу сервера аналитики Domination нужно поставить «галку» на «**Выгружать на сервер фотографии**».



В меню «**Распознавание лиц**» нужно включить распознавание, установив соответствующую «галку».



Далее в меню «**Управление точками доступа**» нужно добавить точку. На вкладке «**Видеонаблюдение**» указать пользовательскую систему, которая была создана. В строке «**Камера**» указать канал распознавания сервера аналитики Domination, на котором будет производиться распознавание лица, и установить «галки» на «**Разрешить верификацию по лицу**» и «**Включить идентификацию по лицу**».



В «**Редактировании режимов допуска персонала**» на «**Уровне 2**» или выше необходимо создать режим с любым названием. На вкладке «**Дни**» на усмотрение администратора создать расписание. На вкладке «**Специальные правила**» в строках «**Верификация лица при проходе «на вход»**» и в «**Верификации лица при проходе «на выход»**» нужно указать жёсткость пропуска. «**Мягкая**» – будет пропускать в любом случае. «**Жёсткая**» – пропустит только в случае, когда карта/ключ совпадут с распознаванием по лицу.