



**VisionLabs**  
MACHINES CAN SEE

# VISIONLABS ACCESS CONTROL

Описание функциональных характеристик  
программного обеспечения

ООО «ВижнЛабс»

123458, г. Москва, ул. Твардовского д. 8, стр. 1

☎ +7 (499) 399 3361

✉ [info@visionlabs.ru](mailto:info@visionlabs.ru)

🌐 [www.visionlabs.ru](http://www.visionlabs.ru)

## Содержание

Глоссарий.....	3
1. Общие сведения о документе .....	5
2. Возможности Access Control.....	6
2.1. Основные возможности Access Control .....	6
2.2. Архитектурные возможности Access Control.....	6
3. Описание работы Access Control.....	7
4. Аппаратные требования .....	8
4.1. Минимальные аппаратные требования.....	8
5. Программные требования .....	9

## Глоссарий

Термин	Определение
Аутентификация	Совокупность мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификатором (идентификаторами) посредством использования аутентифицирующего (аутентифицирующих) признака (признаков) в рамках процедуры аутентификации, в результате чего лицо считается установленным.
Детектирование	Определение области лица на изображении и набора ключевых точек для глаз, носа и рта.
Детекция	Обнаружение лица в кадре.
Идентификация	<p>Совокупность мероприятий по установлению сведений о лице и их проверке, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимым для определения такого лица.</p> <p>В контексте документа – поиск наиболее подходящего БШ путем сравнения полученного БШ с перечнем БШ в базе (сравнение «один ко многим»).</p>
Лучший кадр, лучшая детекция	Лучший кадр выбирается из всех кадров одного трека. Основными условиями выбора лучшего кадра являются приемлемое качество изображения и наличие на нем лица с наилучшим ракурсом. Условия выбора лучшего кадра задаются в настройках Access Control.
Программное обеспечение (ПО)	Программа или множество программ, используемых для управления компьютером.
Портрет	Фрагмент изображения лица с кадра, отобранного в соответствии с настройками алгоритма и максимально приближенный к требованиям ГОСТ 19794-5-2006 / ISO IEC 19794-5 2005(E).
Ракурс	Степень поворота головы (в градусах) по каждой из трех осей вращения (наклон вверх/вниз относительно горизонтальной оси; наклон влево/вправо относительно вертикальной оси; поворот относительно вертикальной оси).
СКУД	Система контроля и управления доступом.
Трансформированное изображение (warp)	Специальный формат изображения для работы с LUNA PLATFORM 5 с выровненным по горизонтали лицом. Такое изображение содержит всю необходимую информацию о лице и при этом быстро обрабатывается системой.

<b>Термин</b>	<b>Определение</b>
Трек	Информация о положении объекта (лица) одного человека на последовательности кадров. Если объект покидает зону кадра, то трек прерывается не сразу. Некоторое время он ожидает возвращения объекта в кадр. Если объект вернулся, то трек продолжается.

## 1. Общие сведения о документе

Программное обеспечение «VisionLabs Access Control» предназначено для реализации механизма идентификации/ аутентификации пользователей и формирования сообщений в СКУД для открытия турникетов/разблокировки магнитных замков на основании результатов распознавания.

VisionLabs Access Control – программное обеспечение, предназначенное для чтения и обработки видеопотоков и отправки изображений лиц в виде HTTP запросов на внешние сервисы.

Интеграция ПО «VisionLabs Access Control» (далее – Access Control) со СКУД позволяет решить следующие задачи:

- контроль доступа;
- повышение удобства прохода и пропускной способности КПП;
- контроль времени пребывания сотрудников и посетителей на охраняемой территории;
- защита от попыток несанкционированного доступа с помощью технологии Liveness<sup>1</sup>.

---

<sup>1</sup> Liveness – программный способ определения, является ли полученная камерой фотография изображением оригинала (лица) или снимком ранее сделанного изображения.

## 2. Возможности Access Control

### 2.1. Основные возможности Access Control

Таблица 1. Основные возможности Access Control

Возможность	Краткое описание
Чтение видеопотоков	Access Control выполняет чтение видеопотоков с камер. В качестве источников данных могут выступать веб-камеры, IP-камеры (посредством протокола RTSP) и видеофайлы.
Обработка видеопотоков	Выполняется поиск и сопровождение лиц в видеопотоке, пока они не покинут кадр или не будут перекрыты.
Детектирование лиц	Процедура нахождения областей изображения, которые содержат лица.
Трекинг лиц	Процедура отслеживания объекта (лица) на последовательности кадров.
Определение качества изображения (выбор лучшего кадра)	Определение качества изображения производится по двум параметрам (задаются в конфигурационном файле): 1. Углы поворота головы относительно центра кадра; 2. Вероятность, позволяющая с высокой скоростью спрогнозировать насколько поступившее изображение подойдёт для последующего сравнения в ПО Access Control Server.
Проверка Liveness	Программный способ, позволяющий подтвердить витальность (живучесть, жизненность) человека по одному или нескольким изображениям с целью предотвращения спуфинг-атак.  Примечание: отправка нормализованного изображения во внешние системы осуществляется только в случае, если результат проверки Liveness положительный
Отсылка изображений лиц в виде HTTP-запросов на внешние сервисы	В качестве внешних сервисов может выступать ПО компании VisionLabs (LUNA PLATFORM ENTERPRISE, LUNA PLATFORM 5, Access Control Server), так и сторонние сервисы, созданные для обработки запросов Access Control. Внешний сервис должен реализовывать RESTful API.

### 2.2. Архитектурные возможности Access Control

1. К одному экземпляру Access Control может быть подключено несколько видеокамер (количество подключаемых источников зависит от аппаратных характеристик сервера и рассчитывается на этапе технического проектирования).
2. Возможность масштабирования Access Control за счёт использования сразу нескольких экземпляров Access Control.

### 3. Описание работы Access Control

1. В Access Control отправляется видео с камеры видеонаблюдения, веб камеры или видеофайл. Access Control может работать сразу с несколькими источниками видеопотока;
  2. Access Control детектирует лица на каждом отдельном кадре каждого видеопотока. Для каждого нового лица в потоке создается трек, который подкрепляется новыми детекциями данного лица с последующих кадров;
  3. Access Control отсекает кадры плохого качества. В зависимости от настроек для каждого трека выбирается лучшая детекция в треке или несколько детекций;
  4. На основе кадра с лучшей детекцией формируется портрет или трансформированное изображение с найденным лицом;
  5. Портрет (трансформированное изображение) отправляется на внешний сервис в виде HTTP запроса.
- Существует несколько алгоритмов выбора лучшей детекции/детекций в треке. Эти алгоритмы задаются с помощью параметров запуска. Например, для отправки кадра на сервер может выбираться детекция с максимальной оценкой.

## 4. Аппаратные требования

### 4.1. Минимальные аппаратные требования

Для корректной работы приложения аппаратное обеспечение должно отвечать следующим минимальным требованиям:

- CPU с частотой 2 Гц и выше;
- 4 Гб оперативной памяти и выше;
- 400 Мб свободного места на жестком диске.

На аппаратные требования влияют несколько факторов:

- Количество обрабатываемых видеопотоков;
- Частота и разрешение кадров видеопотоков;
- Параметры настройки Access Control. Настройки по умолчанию являются наиболее универсальными. В зависимости от условий эксплуатации приложения с помощью их значений можно повлиять на качество или производительность.

Access Control также может работать в режиме ускорения вычислений за счет:

- Использования AVX-инструкций;

Для использования требуется CPU с поддержкой AVX. Система автоматически определяет наличие инструкций и запускается в наиболее оптимальном режиме;

- Использования ресурсов видеокарты;

В таком случае требуется видеокарта NVIDIA с поддержкой CUDA, не менее 2 Гб RAM. Поддерживаются архитектуры Kepler, Maxwell, Pascal.

## **5. Программные требования**

Access Control может работать под управлением следующих операционных систем:

- CentOS Linux Release 7.3 x86\_64;
- Windows (64-bit) 7, 8.1, 10 (с установленным пакетом C++ Microsoft Redistributable 2015).