



КОНТРОЛЬ ДОСТУПА НА ОСНОВЕ РАСПОЗНАВАНИЯ ЛИЦ.

ИНФОРМАЦИОННЫЙ ДОКУМЕНТ,
ПОДГОТОВЛЕННЫЙ BOON EDAM

**BOON EDAM**
YOUR **ENTRY** EXPERTS.



ВВЕДЕНИЕ.

Данный информационный документ описывает принципы работы контроля доступа на основе распознавания лиц. В нём также представлены факторы, которые следует учесть при выборе соответствующей системы контроля доступа. Поскольку технология распознавания лиц появилась на рынке недавно, вам будет интересно познакомиться с важными аспектами её применения. Ознакомление с информационным документом позволит лучше понять, как осуществляется контроль доступа на основе распознавания лиц и на что следует обратить внимание при покупке такой системы.

ВИДЫ БИОМЕТРИЧЕСКИХ ДАННЫХ

Биометрические идентификаторы — это измеряемые характеристики, которые можно использовать для описания людей. Биометрические данные всё чаще используются в решениях для контроля доступа. Наибольшее распространение получили четыре вида биометрического контроля:

СКАНИРОВАНИЕ СЕТЧАТКИ ГЛАЗА

Сетчатка глаза каждого человека уникальна. Специальный сканер распознаёт углубления, складки и бороздки в радужной оболочке и преобразует их в цифровой код. Затем этот код проверяется по базе данных, и система определяет, предоставлять человеку доступ или нет.

ИДЕНТИФИКАЦИЯ ПО ВЕНАМ ЛАДОНИ

В инфракрасных лучах ближнего диапазона виден уникальный рисунок вен и капилляров ладони. Некоторые сканеры также способны измерять складки и узелки. На основе этой информации создаётся уникальный профиль авторизованного лица.

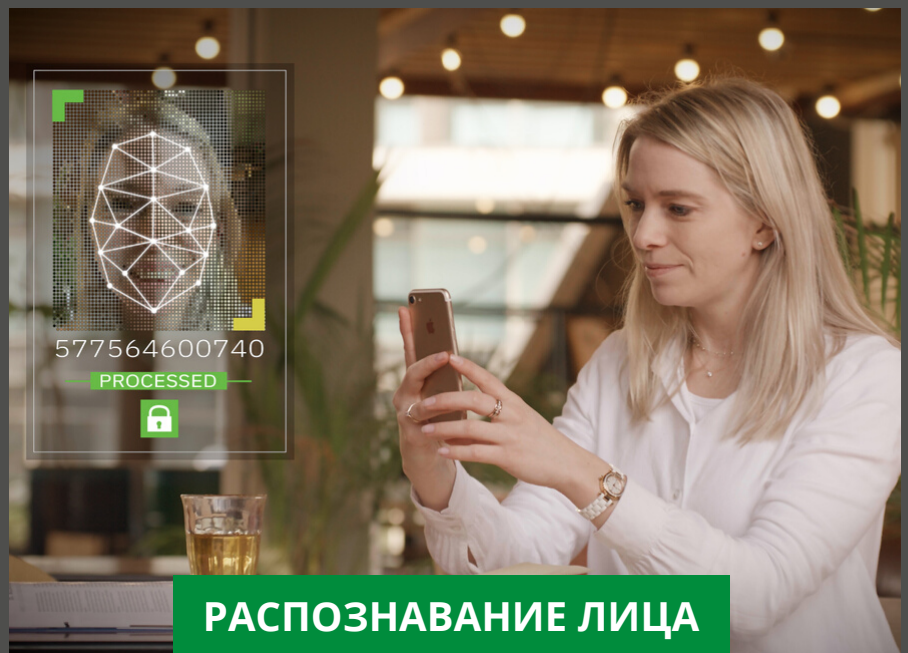
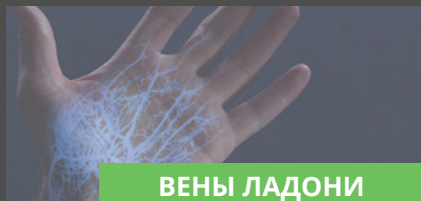
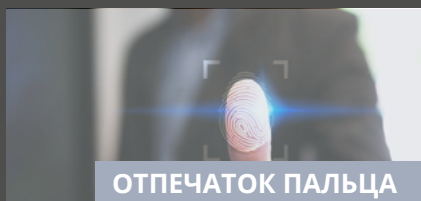
ИДЕНТИФИКАЦИЯ ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ

Существуют различные виды сканеров отпечатков пальцев. Все они регистрируют уникальный узор папиллярных линий на коже. Полученные данные используются для вынесения решений о предоставлении доступа.

РАСПОЗНАВАНИЕ ЛИЦ

Последний вид биометрического контроля доступа основан на технологии распознавания лиц. Специальный алгоритм выделяет лицо человека на видео или фотографии. Всего за несколько миллисекунд система регистрирует характеристики лица и преобразует их в уникальный код.

Затем программное обеспечение для распознавания сравнивает этот код с содержимым базы данных. При обнаружении соответствия происходит идентификация человека на снимке и выносится решение о предоставлении доступа.





РАСПОЗНАВАНИЕ ЛИЦ

Распознавание лиц может использоваться для решения различных задач. Данный информационный документ описывает использование этой технологии для контроля доступа. Различия областей применения кратко представлены ниже.

МАССОВОЕ ВИДЕОНАБЛЮДЕНИЕ

В системах массового видеонаблюдения распознавание лиц используется для идентификации людей в толпе. Для получения надлежащих результатов необходимо специализированное оборудование и мощное ПО.

ПЕРСОНАЛЬНАЯ АУТЕНТИФИКАЦИЯ

Этот вид распознавания лиц обычно используется в мобильных устройствах (например, смартфонах), требования к ПО и оборудованию при этом невысоки. В данном случае лицо используется вместо пароля.

СУДЕБНАЯ ЭКСПЕРТИЗА

Распознавание лиц может применяться для реконструкции передвижений конкретного человека по видеозаписям. Например, такие данные помогают установить, в каких местах индивид, скрывающийся от правосудия, был замечен за последние 24 часа.

КОНТРОЛЬ ДОСТУПА

Наконец, распознавание лиц используется для контроля доступа. Для этого необходимо настроить программное обеспечение, которое будет сравнивать информацию с несколькими видеокамер с содержимым базы данных в режиме реального времени. В зависимости от размера базы данных устанавливается сервер, который будет подтверждать авторизацию с достаточной скоростью и открывать точку доступа.

СОДЕРЖАНИЕ ИНФОРМАЦИОННОГО ДОКУМЕНТА:



**ПРЕИМУЩЕСТВА
ТЕХНОЛОГИИ
РАСПОЗНАВАНИЯ ЛИЦ**



**КОМПОНЕНТЫ
ТЕХНОЛОГИИ
РАСПОЗНАВАНИЯ ЛИЦ**



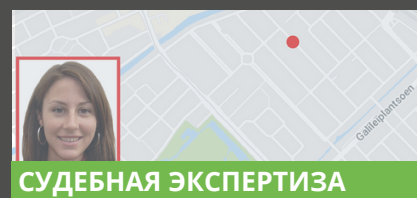
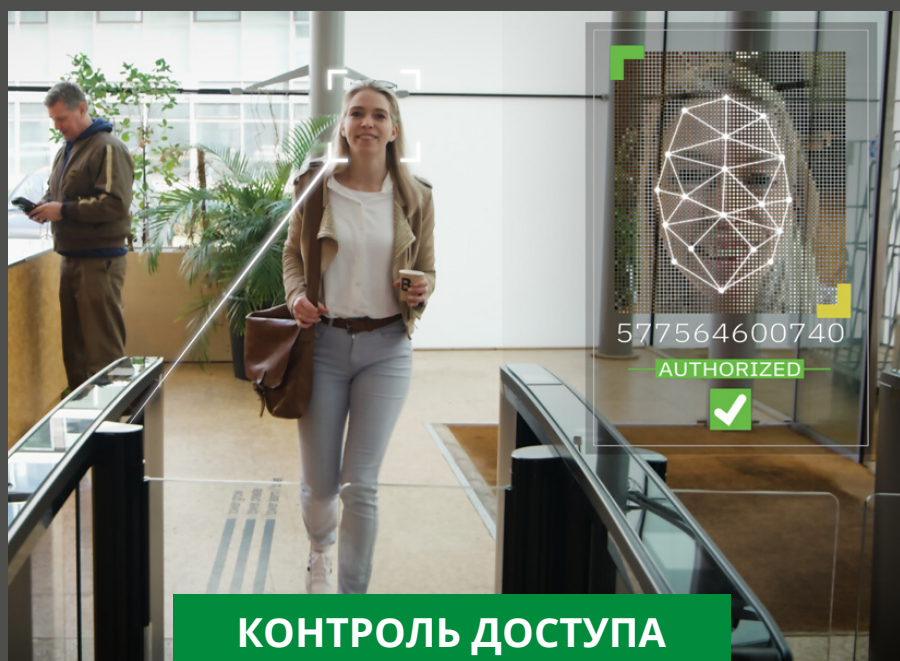
**ТЕХНИЧЕСКИЕ
ХАРАКТЕРИСТИКИ**



**ПРАКТИЧЕСКОЕ
ПРИМЕНЕНИЕ**



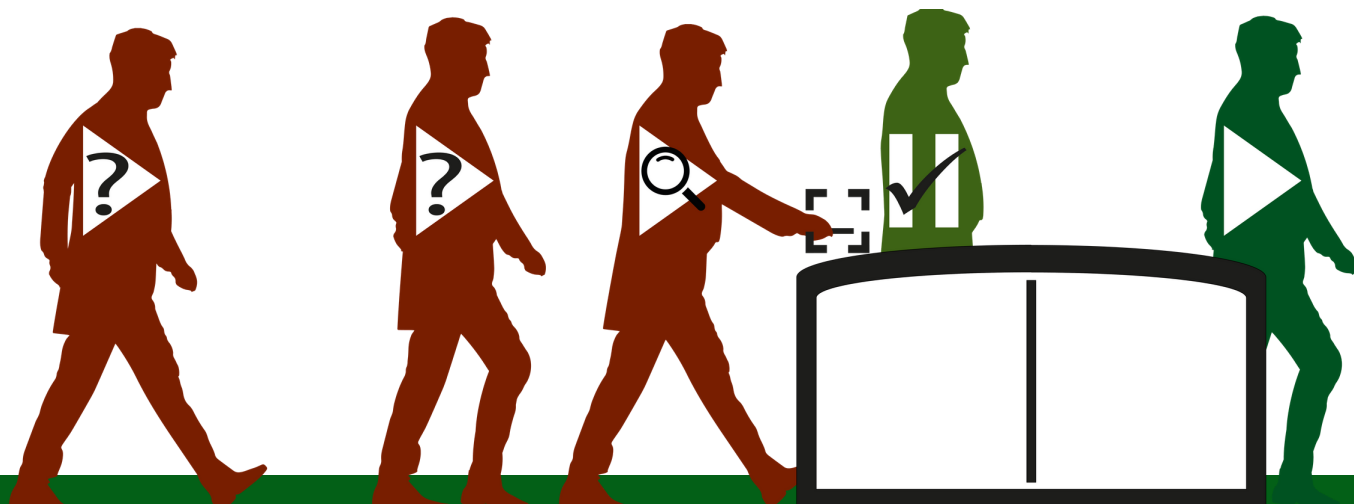
**ЦИФРОВАЯ
БЕЗОПАСНОСТЬ**



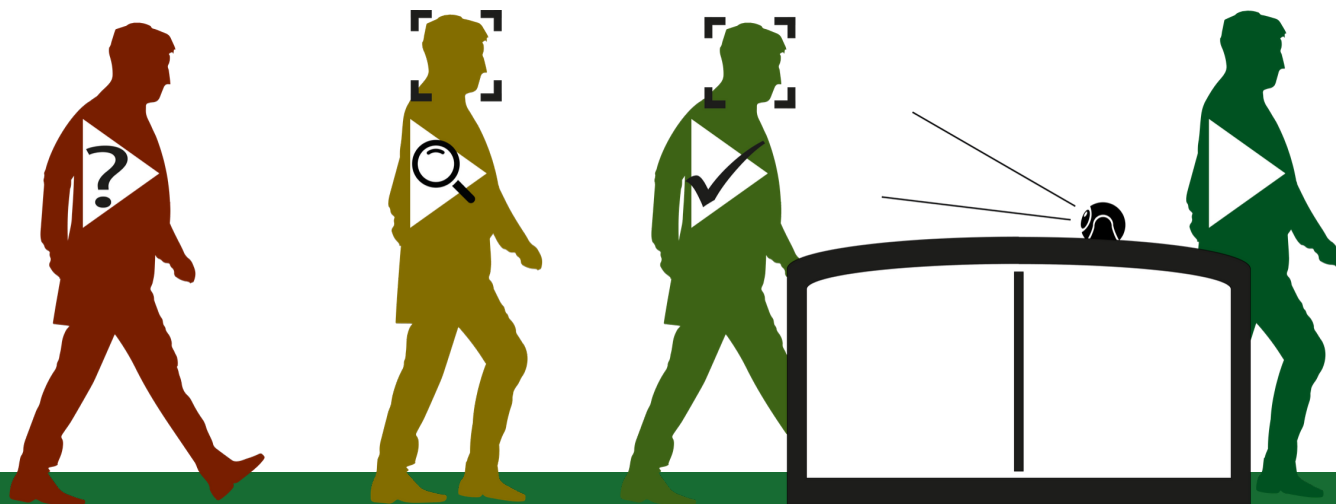


ПРЕИМУЩЕСТВА ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ЛИЦ.

«ТРАДИЦИОННОЕ» УСТРОЙСТВО ДЛЯ СЧИТЫВАНИЯ КАРТ



РАСПОЗНАВАНИЕ ЛИЦ



УЛУЧШЕНИЕ ПРОХОДИМОСТИ

Одно из главных преимуществ контроля доступа на основе распознавания лиц — отсутствие очередей. Программное обеспечение регистрирует лицо человека уже на подходе к турникету и примет решение о предоставлении доступа к моменту его прибытия в точку прохода. Авторизованное лицо сможет сразу пройти через открытый системой проход. При этом лица без прав доступа не смогут незаметно проникнуть на территорию объекта через этот вход. Проход через точку доступа станет простым и беспрепятственным.



БЫСТРЫЙ ДОСТУП В ЛЮБОЕ ВРЕМЯ

Поскольку при биометрическом контроле на основе распознавания лиц человеку не требуется носить с собой дополнительные средства идентификации, он никогда не окажется перед закрытой дверью. Все лица уникальны, и их черты позволяют отличить одного человека от другого и идентифицировать их.

Ещё одно преимущество технологии заключается в том, что она почти не требует от пользователя активного взаимодействия с точкой контроля доступа. Как только лицо попадает в фокус камеры, ПО приступает к авторизации. Отпадает потребность в пропусках, забыть их также не получится. Кроме того, сотрудникам не придётся ждать, пока коллега роется в вещах в поисках пропуска, и они смогут свободно держать в руках верхнюю одежду и сумки.

ИСКЛЮЧЕНИЕ ПЕРЕДАЧИ ПРОПУСКОВ

Распространённая проблема при контроле допуска — передача персональных пропусков коллегам. Такое ненадлежащее использование может стать причиной проникновения на объект людей, не имеющих на то права. Распознавание лиц полностью исключает прохождение посторонних через точку доступа.

Кроме того, контроль доступа на основе распознавания лиц снимает проблему украденных пропусков или их дубликатов. В результате повышается общий уровень защищённости.



БЕСКОНТАКТНАЯ БИОМЕТРИЯ

Многие люди на мгновение замирают перед сканированием сетчатки или пальца. Такая пауза возникает непроизвольно из-за недостаточного знакомства с системой или нежелания добровольно подставлять свою часть тела под сканер. С одной стороны, это нарушает проходимость точки доступа, а с другой, создаёт ощущение, что система контроля недостаточно дружелюбна по отношению к пользователю.

Важное преимущество технологии распознавания лиц заключается в том, что она регистрирует данные пользователя на расстоянии с помощью видеочкамеры. Пользователям не приходится принимать неудобное положение или касаться точки доступа. Как только они окажутся в выбранной зоне действия видеочкамеры, система выполнит идентификацию и позволит им свободно осуществить проход.



КОМПОНЕНТЫ ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ЛИЦ.

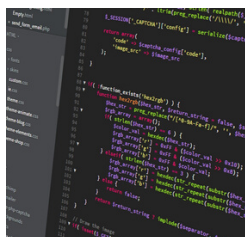
При внедрении контроля доступа на основе распознавания лиц необходимо учесть, что такая система состоит из нескольких компонентов. Эти взаимодействующие друг с другом компоненты часто поступают от различных поставщиков. По этой причине необходимо тщательно изучить, оборудование каких производителей позволит построить безупречно функционирующую систему. В общем случае она предполагает взаимодействие следующих компонентов:



ВИДЕОКАМЕРЫ И ДРУГИЕ ДАТЧИКИ

Видеокамера — важный элемент, обеспечивающий надёжное срабатывание ПО для распознавания лиц. На рынке доступны различные высококачественные устройства этого типа. Опыт показывает, что для оптимального выбора удобного и дружелюбного к пользователю устройства необходимо учесть технические и эстетические факторы.

Количество мегапикселей — не единственная характеристика. Следует учесть и такие важные показатели, как светочувствительность, вид линзы и вычислительная мощность процессора. Чтобы система отличала реальные лица от фотографий, можно установить дополнительные датчики.



ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РАСПОЗНАВАНИЯ ЛИЦ

Программное обеспечение для распознавания лиц является центральным элементом системы. Оно преобразует черты лица в цифровой код для сопоставления с имеющейся базой данных. Распознавание достигается путём применения серии алгоритмов. Программное обеспечение для распознавания лиц часто работает автономно от других программ для контроля доступа. Это позволяет создать отдельную систему, запускающую ПО на внешнем процессоре.

Важно обеспечить соответствие программного обеспечения и системы требованиям Федерального закона о персональных данных и внедрить надлежащие стандарты шифрования.



СИСТЕМА КОНТРОЛЯ ДОСТУПА

В системах контроля доступа часто используется несколько программных решений. Их интеграция обычно осуществляется с помощью системы управления безопасностью или зданием. По этой причине ПО для распознавания лиц должно быть также совместимо с этой системой.

На практике это обеспечивается подключением различных модулей, которые затем управляются через единую централизованную программу. В таком случае интеграция модуля «ПО для распознавания лиц» будет выполняться через интерфейс API.



ФИЗИЧЕСКИЙ ДОСТУП

В системах контроля доступа технология распознавания лиц всегда используется в сочетании с решением для контроля физического доступа. Именно физический барьер препятствует проникновению на объект посторонних. Доступны различные варианты барьеров, которые обеспечивают определённый уровень защищённости.

Существует несколько вариантов конфигурации. Например, можно приобрести системы физического контроля с интегрированной технологией распознавания лиц или заказать компоненты по отдельности.



ТЕХНИЧЕСКИЕ АСПЕКТЫ.



ОСВЕЩЕНИЕ

Одно из главных условий успешного распознавания лиц — достаточная освещённость зоны, в которой находится камера. При контроле доступа такое распознавание часто производится внутри помещений, поэтому освещённость можно легко отрегулировать.

Серьёзную проблему представляет избыточная выдержка (засветка). Её источниками могут стать яркий солнечный свет, блики отражений или высокие стеклянные потолки. Видеокамеры и ПО для распознавания лиц нередко с трудом реагируют на изменения освещённости.

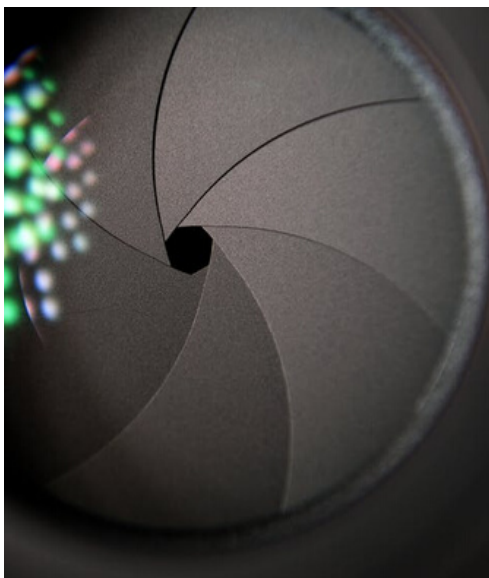
Недостаточную выдержку исправить намного легче. Для улучшения качества распознавания часто достаточно отрегулировать настройки камеры. Для решения этой задачи рекомендуется привлечь эксперта.

РАЗМЕЩЕНИЕ ВИДЕОКАМЕРЫ

При установке видеокамеры следует учитывать качество записываемого ею изображения. Чем ближе камера к человеку, которому требуется доступ, тем выше будет качество картинки.

Также следует учесть расположение камеры по отношению к пользователю. Лучше всего установить камеру так, чтобы пользователь изначально смотрел в этом направлении, готовясь к прохождению через точку доступа. В этом случае ему не придётся совершать дополнительных действий для идентификации.

Кроме того, видеокамеру можно интегрировать в решение для контроля доступа либо установить её снаружи из эстетических соображений.



ФОКУС ВИДЕОКАМЕРЫ

При установке видеокамеры обратите особое внимание на фокус. Он должен приходиться на место сканирования лица. Фокусное расстояние от точки доступа не должно быть слишком большим (чтобы исключить тайное проникновение посторонних) или чрезмерно коротким (во избежание длительного ожидания).

Фокус видеокамеры также определяет диапазон, внутри которого происходит распознавание лиц. Для его настройки выберите соответствующую область изображения в программном обеспечении.

Наши эксперты с радостью помогут вам определить подходящие технические характеристики с учётом конкретной ситуации.

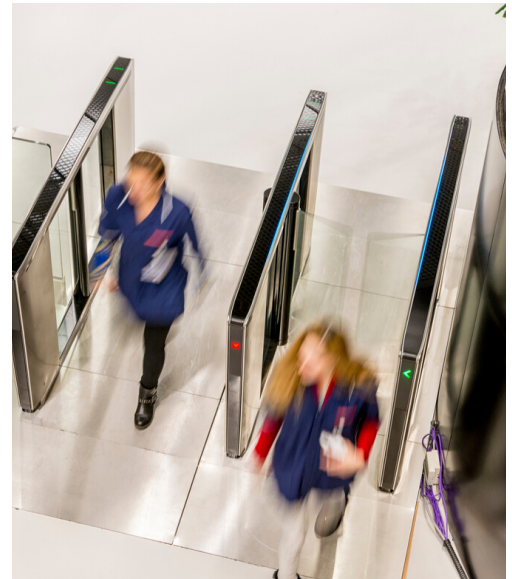


ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ.

ПОТОК ПОЛЬЗОВАТЕЛЕЙ

На практике использование скоростных турникетов естественным образом настраивает пользователей принимать положение лицом вперёд. Люди проходят через них по прямой и глядя перед собой. В результате возникает довольно ограниченная в размерах зона, в которой будут находиться все лица пользователей.

Ещё одно важное преимущество доступа на основе распознавания лиц — улучшение потока пользователей. Все сотрудники проходят через скоростной турникет равномерно и в одном направлении. Распознавание лиц обеспечивает достаточно высокую скорость аутентификации для поддержки такого оптимального потока.



ПОКАЗ ЛИЦА

Выше в информационном документе отмечалось, что при контроле доступа на основе распознавания лиц пользователю не нужно выполнять дополнительных действий. Однако это зависит от степени осознания пользователем того факта, что специальное ПО должно иметь возможность просканировать его лицо.

На практике сотрудники должны показывать своё лицо видеокамере в более или менее узнаваемом виде. Например, они не смогут пройти через точку доступа закутавшись в шарф или обернувшись назад. Чтобы система работала, пользователи должны сотрудничать с ней.

ВЗАИМОДЕЙСТВИЕ С ПОЛЬЗОВАТЕЛЕМ

При использовании технологии распознавания лиц и контроля доступа в целом важна качественная обратная связь для пользователей. Когда через точку доступа быстро один за другим проходят несколько человек, для сообщения решений ПО можно использовать визуальные и звуковые сигналы.

Распознавание лиц хорошо подходит для ситуаций с большим количеством проходов одних и тех же пользователей. После первичной регистрации авторизованному лицу предоставляется доступ на необходимое время. Постоянные пользователи постепенно привыкают к взаимодействию с системой контроля доступа.





ЦИФРОВАЯ БЕЗОПАСНОСТЬ.



ШИФРОВАНИЕ

Чтобы предотвратить хищение данных и изображений при их передаче по сети, в ПО для распознавания лиц применяется шифрование. Шифрование предполагает кодирование цифровой информации (изображения). Без знания особенностей процесса шифрования посторонние лица не смогут выполнить чтение данных.

Существуют различные методы шифрования данных. Выбор наиболее подходящего решения будет зависеть от имеющейся инфраструктуры и программной платформы управления видео. Например, имеет значение, передаются ли данные по закрытой или открытой сети. Наши эксперты с радостью ответят на любые ваши вопросы по этой теме.

ОБНАРУЖЕНИЕ МОШЕННИЧЕСТВА

Технология распознавания лиц постоянно развивается для более эффективного обнаружения мошенничества. Цель такого совершенствования — предотвратить случаи обмана системы, например путём поднесения к видеокамере фотографии. На сегодняшний день имеются два метода обнаружения и предотвращения мошенничества:

- Обнаружение с помощью аппаратных средств — 3D-датчиков, сканирующих строение лица. Один из вариантов — регистрация датчиком узора цветных лучей света, отражённых лицом.
- Обнаружение с помощью программных средств, которые улавливают мельчайшие отклонения на видеоизображении. Для этого необходимы большие вычислительные возможности (для обработки видео), а следовательно — более крупные и мощные серверы.



ЗАКОНОДАТЕЛЬСТВО

Выше в информационном документе упоминалось, что для распознавания лиц используются биометрические данные. Важно понимать, что с точки зрения законодательства они составляют особую категорию персональных данных. Биометрические характеристики могут использоваться для персональной идентификации при определённых условиях. Данные необходимо применять исключительно для аутентификации или с целью обеспечения безопасности. Кроме того, системный администратор должен иметь возможность подтвердить, что обработка данных отвечает требованиям законодательства. В этом случае использование технологии распознавания лиц для контроля доступа будет законным.



ЗАКЛЮЧЕНИЕ.

Цель настоящего информационного документа — представить базовые сведения о контроле доступа на основе распознавания лиц и факторах выбора наиболее подходящей системы этого вида для вашей компании. В документе раскрываются различия между видами биометрических данных и методами распознавания лиц. Кроме того, в нем описаны преимущества технологии распознавания лиц по сравнению с традиционными системами контроля доступа.

Рассматриваются также компоненты систем распознавания лиц для контроля доступа и их наиболее важные технические и практические аспекты. Наконец, в информационном документе кратко говорится о применении распознавания лиц в контексте цифровой безопасности и действующего законодательства.

РЕКОМЕНДАЦИИ

В данном информационном документе компания Boon Edam представила основные сведения об условиях и требованиях к внедрению распознавания лиц. Мы считаем, что эта технология хорошо зарекомендовала себя за последние годы и что в будущем её использование будет только расширяться. Кроме того, важно упомянуть, что контроль доступа на основе распознавания лиц подходит практически для всех уровней безопасности. Мы будем рады помочь вам в выборе и внедрении оптимальной системы с учётом ваших нужд, пожеланий и конкретных обстоятельств (количества людей, распознаваемых системой, расположения точек доступа и т.д.).

Чтобы получить дополнительные сведения о контроле доступа на основе распознавания лиц, свяжитесь с автором информационного документа или другим экспертом Boon Edam. Мы будем рады встретиться с вами для предоставления ни к чему не обязывающей консультации.

Часто задаваемые вопросы.

Когда я, как пользователь, подхожу к точке доступа с системой распознавания лиц, она кодирует характеристики моего лица и сравнивает их с содержимым базы данных. Означает ли это, что в системе останется моя фотография?

Нет, для создания базы данных не требуется сохранение лиц пользователей, достаточно списка хэш-кодов. Решение для контроля доступа также не требует хранения фотографий с целью сравнения. При этом на практике системы распознавания лиц могут иногда на короткое время сохранять фотографии для оптимизации ПО. Эти снимки находятся на автономном сервере и недоступны для посторонних лиц.

Сохраняет ли система другие данные, помимо хэш-кода?

В большинстве случаев традиционные системы контроля доступа регистрируют время входа авторизованного пользователя в помещение. Ту же операцию выполняют и системы распознавания лиц. Чтобы исключить сохранение этих данных, достаточно изменить настройки.

Можно ли использовать распознавание лиц с другими входными решениями, помимо турникетов?

Да, эта технология распознавания лиц совместима со многими другими входными решениями. Будем рады обсудить с вами все возможные варианты.

ГЛОБАЛЬНОЕ ПРИСУТСТВИЕ.

Более 140 лет мы занимаемся производством надёжных и безопасных решений премиум-класса для контроля доступа в Нидерландах, США и Китае. Можно с уверенностью сказать, что наши филиалы действуют по всему земному шару. В странах, где нет собственного представительства Boon Edam, наше международное экспортное подразделение заключает партнёрские соглашения с эксклюзивными дистрибьюторами или предлагает решения и услуги напрямую. Благодаря такому присутствию мы хорошо знаем ситуацию на местных рынках и их уникальные потребности в плане входных решений.

Для поиска ближайшего специалиста Boon Edam перейдите по этой ссылке:
www.boonedam.ru/touchless



Boon Edam LLC

T +7 495 223 89 69

E ru.info@boonedam.com

B www.boonedam.ru


BOON EDAM
YOUR ENTRY EXPERTS.