Современные тенденции в развитии биометрических терминалов контроля доступа.

Обзор мнений и решений

Материал подготовлен при активном участии Василия МАМАЕВА, заместителя директора некоммерческого партнерства «Русское биометрическое общество»

Мы попросили экспертов ответить на следующие вопросы:
1. Современные тенденции в развитии биометрических терминалов контроля доступа (БТКД).
2. Портрет заказчика БТКД. Сегменты рынка.
3. Характерные особенности современных БТКД.

Владислав ШАПОВАЛОВ,
начальник отдела маркетинга официального представительства «ZKTeco - Биометрия и безопасность»

1. Биометрические технологии идентификации с каждым годом все больше и больше вытесняют старые методы, такие как пароль, RFID-карта и подобные. Биометрия имеет ряд преимуществ: степень защиты в разы выше, ее практически невозможно подделать и скопировать, ее нельзя забыть (как, например, пароль) или потерять (как карту).

Увеличение мощности современных процессоров позволило производителям биометрического оборудования использовать более совершенные методы и от простого сканера отпечатка пальца или рисунка ладони перейти к распознаванию лиц. Более того, современные алгоритмы позволяют распознавать сразу несколько лиц в потоке, при движении объекта под разными углами относительно камеры и даже при плохой освещенности. Многие компании начали использовать гибридную идентификацию – сочетание двух и более вышеперечисленных методов. И это только одна технология – статическая. Она основана на физиологических особенностях человека. Весьма бурно развиваются и динамические технологии. Они основаны на поведенческом анализе движений, походки, манере письма, поведения за компьютером или мобильным устройством, интонациях и тембре голоса. Эти методы сложнее и требуют больших вычислительных ресурсов, но вероятность подделки при их использовании сводится к нулю. Примером их реализации являются широко известные Windows Hello, Google Hands Free Payments, Apple TouchID.

G4 Автономный мультибиометрический терминал (ZKTeco)

Терминал с инновационным алгоритмом распознавания лиц ZKTeco, сенсором отпечатка пальца SilkID и считывателем RFID-карт. Устройство может выполнять идентификацию на расстоянии 0,5-3 м и работает автоматически при обнаружении лиц, обеспечивает высокую скорость (<0.5 сек) и точность распознавания. Благодаря алгоритму глубокого самообучения значительно улучшена устойчивость распознавания, уменьшена зависимость от расположения объекта (±30 градусов), встроена защита от поддельных идентификаций. Кроме того, терминал способен идентифицировать сухие, мокрые или грубые поверхности пальцев. Он может быть подключен к турникетам или дверям в учебных заведениях, офисных центрах, предприятиях среднего и крупного бизнеса, интегрирован в сложные системы. Имеются все необходимые интерфейсы для управления одной дверью: дверной замок, AUX вход/выход, кнопка выхода, дверной датчик, звонок. Связь: TCP/IP, USB хост, Wiegand вход/выход. Экран 7" TFT.

2. Усовершенствования в технологии биометрической идентификации изменили и рынок систем безопасности. Если раньше сегмент, занимаемый биометрией, был очень узок и в основном распространялся на системы безопасности наивысшего класса, то сейчас достаточно низкая цена оборудования позволяет применять такие устройства в средних и даже небольших проектах. Биометрия заинтересовала банки. Например, ПАО «Сбербанк» активно развивает это направление, устанавливая биометрические сканеры в своих терминалах. Одновременно Сбербанк развивает проект «Ладошки» — это идентификация по рисунку ладони в школах в терминалах оплаты обедов. То, что производители стали выпускать автономные биометрические терминалы и добавили в них функцию ведения табеля учета рабочего времени, еще больше расширило возможности их применения. Теперь руководитель любой компании может приобрести такое устройство и, установив у себя в офисе, решить сразу две задачи – контроль доступа и контроль рабочего времени персонала. Таким образом, рынок биометрии меняется и расширяется, в него вовлекаются все новые и новые участники из разных сфер бизнеса.

3. Современные биометрические терминалы можно разделить на группы по типу идентификации: по отпечатку пальца, по рисунку вен пальца, по рисунку ладони, по рисунку сетчатки глаза и, наконец, с идентификацией по лицу. Есть гибридные устройства, сочетающие сразу несколько видов из вышеперечисленных, также производители для большей универсальности добавляют считыватель RFID-карт и возможность ручного ввода ID посетителя и пароля. Терминалы выпускают в автономном исполнении или же они работают в связке с контроллером, который обрабатывает полученные данные и хранит все необходимые шаблоны. Такая схема иногда оказывается удобнее, так как контроллер может работать сразу с несколькими терминалами. Это позволяет установить более дешевые терминалы-считыватели, решить проблему быстрой синхронизации профилей посетителей сразу на всех терминалах и интегрировать в систему контроля доступа и безопасности. Многие автономные терминалы имеют функцию учета рабочего времени и оборудованы системой контроля доступа. Они могут управлять электронным замком двери, отслеживать состояние двери, управлять звонком и кнопкой выхода. Наличие AUX входов и выходов позволяет подключать датчики дыма и систему тревожной сигнализации. В некоторых из них имеется батарея резервного питания. Также производители начали выпускать терминалы, сразу интегрированные в замок – так называемая система «умный замок». Устройство сделано как замок с двумя ручками, щеколдой и легко устанавливается вместо обычного механического замка. Большое распространение такие системы получили в гостиничном бизнесе.

Некоторые производители выпускают специализированное программное обеспечение, позволяющее значительно расширить функциональность системы: организовать работу с большим количеством биометрических считывателей, упростить процесс создания, удаления, резервного копирования и синхронизации профилей посетителей. Для работы с ПО достаточно подключить терминалы в обычную компьютерную сеть. Специальные программные модули позволяют адаптировать систему для конкретного бизнеса. Например, для гостиничного бизнеса добавить функцию регистрации и хранения данных о гостях отеля, разрешить перемещение только внутри разрешенных зон здания, отслеживать текущее положение и пр. В другой сфере, например, в бизнес-центре, можно организовать доступ соответствующих лиц только на заданные этажи в заранее указанное время, добавить модуль управления доступом на парковку и т. д. Подключение к сети позволяет управлять системой через интернет из любой точки планеты.

Андрей ТУЖИЛКИН,
начальник отдела программного обеспечения
ЗАО «АЛГОНТ»

– Изначально биометрические терминалы контроля доступа (БТКД) применяли как системы безопасности, определяющие право доступа сотрудников и ограничивающие попытки несанкционированного пребывания. Со временем появились системы управления предприятием, в которые интегрировались БТКД с дополнительным функционалом управления рабочим временем. Если раньше основными потребителями таких систем были крупные промышленные и коммерческие компании, то теперь, с увеличением числа бизнес-центров, даже небольшие компании устанавливают системы контроля доступа для обеспечения безопасности и контроля ресурсов. Цель любой компании – получение прибыли, для этого, в первую очередь, необходимо снижать издержки и управлять рисками. БТКД как часть системы безопасности дают возможность эффективно контролировать перемещение сотрудников и трудовую дисциплину. Автоматизация позволяет составить наиболее полную картину эффективности рабочего процесса, выявить узкие места и неэффективных сотрудников, а главное – исключается человеческий фактор.

Интересы работодателя не всегда соответствуют интересам сотрудников или конкурирующих организаций, поэтому такие системы чаще всего пытаются скомпрометировать путем подмены данных. Широко применяемые в настоящее время карты доступа не обеспечивают полную идентификацию личности сотрудника, возможна передача карты, ее дублирование. Использование БТКД позволит решить эту проблему путем верификации карты и личности или отказа от карт-пропусков и перехода на биометричес-

Консоль распознавания «АССаД-ID» (АЛГОНТ)

Консоль распознавания «АССаД-ID» предназначена для использования в составе систем контроля и управления доступом для идентификации персонала по изображению лица с функцией защиты от прохода по фотографии или видеоизображению с планшета и автоматической регулировкой для распознавания абонентов разного роста в диапазоне от 150 до 195 см.

Консоль может быть использована как средство идентификации в любом пропускном пункте СКУД: кабине, турникете, двери.

Сертификат по требованиям безопасности информации №РОСС RU.0001.БИ00 до уровня обрабатываемой информации «секретно» включительно. Высокая точность и скорость распознавания. Бесконтактный способ распознавания абонентов. Контроль роста абонентов. Защита от фальсификации (по фотографии или видеоизображению). Поддержка функций верификации и идентификации в одном устройстве. Интеграция с любыми СКУД. Встроенная LED-подсветка с дополнительной функцией индикации состояний консоли.

кую идентификацию. Это ускорит время прохода человека через проходную, а также позволит вести точный учет рабочего времени и местонахождения сотрудника в любой момент, контролировать простои и опоздания.

К биометрическим параметрам относятся отпечаток пальца, радужная оболочка глаза, голос, лицо, почерк. Наиболее часто используется технология сканирования отпечатка пальца в связи с простотой получения и идентификации, но эта технология несовершенна и существует множество способов ее обойти. Из перспективных технологий, призванных заменить отпечаток, в связи с минимальным взаимодействием с человеком и наибольшей скоростью работы наиболее часто используется технология распознавания лиц. При этом она наиболее уязвима для атак – любую качественную фотографию или видео можно использовать для фальсификации. Защитой от подобных атак выступает технология «контроля живучести» (liveness detection), которая стала неотъемлемой частью современных систем биоидентификации. Методы реализации liveness detection делятся на программные и аппаратные.

Программные методы обрабатывают изображение, получаемое с обычной RGB камеры, установленной на уровне лица. Анализу подвергается видеопоток (динамический метод) или одиночное изображение (пассивный метод). Первый тип подразумевает анализ движений лица (мимика, микроколебания), что требует определенного участия человека в процессе распознавания и, тем самым увеличивает время распознавания до нескольких секунд, что при необходимости идентификации большого количества людей приведет к скоплениям у БТКД. К тому же существует возможность фальсификации путем демонстрации видеозаписи лица на экране планшета. Пассивные методы чаще всего используют преобразования Фурье или анализ текстуры лица. Минусами этого подхода является большая зависимость от качества освещения и возможность обхода с помощью изображения с экрана планшета в высоком разрешении.

Аппаратный метод liveness detection основывается на использовании специальных камер (в основном тепловых и 3D-камер), позволяющих получить дополнительное изображение (тепловую карту или карту глубин, соответственно). Данный подход практически не зависит от условий освещения, «проверка живучести» проходит практически мгновенно, а так же отличается высокой защитой от фальсификаций (обман системы возможен применением точной текстурированной 3D модели головы с имитацией теплового рисунка лица). К недостаткам относится необходимость использования дополнительной специальной камеры.

На практике в современных БТКД применяют комплексный подход к биоидентификации. Использование одного метода не дает полной гарантии от несанкционированного доступа. Чаще всего используются программно-аппаратные методы liveness detection или введение второго биометрического фактора (голос, отпечаток пальца, анализ кровотока, рост и вес).

Главной задачей в развитии современных систем биоидентификации будет повышение защиты от фальсификации. Адаптация к угрозам и повышение безопасности ведет к повсеместному внедрению таких систем.

Вадим КОЛОМИЕЦ,
директор по развитию бизнеса компании «Сонда»

– Биометрические СКУД (далее БиоСКУД) с использованием отпечатка пальца в виде идентификатора появились на рынке систем безопасности более 10 лет назад. Рынок был заполнен большим количеством низкокачественных систем, которые только дискредитировали само понятие «биометрия». Российские компании, которые занимались немногочисленными внедрениями БиоСКУД, пытались приспособить относительно дешевые биометрические сканеры к разработанным российским

БиоСКУД СОНДА (СОНДА)

БиоСКУД СОНДА построена по серверной архитектуре. На сервере:
- создается база данных с шаблонами отпечатков пальцев с АРМ регистрации;
- формируются математические шаблоны из изображений отпечатков пальцев, полученных от терминалов АСД-7;
- принимается решение на пропуск через турникет по результатам сравнения текущего шаблона с шаблоном, хранящимся в базе данных.
Терминал АСД-7 состоит из двух оптических головок и контроллера, не имеет органов управления. Терминал АСД-7 имеет двухканальное управление контроллера турникета на вход и выход. На терминале могут быть установлены считыватели карт по требованию заказчика (EM-Marine, Mifare). Все настройки производятся с помощью ПО СОНДА.
Оптический сканер имеет размер 25х18 мм, разрешающая способность – до 1000 dpi, матрица 1,3 Мп, питание 5В, размеры 110х93х85 мм.
Система внедрена и эксплуатируется на предприятиях с численностью 10 тысяч человек и более, а также в учебных заведениях (школах, студенческих общежитиях).
БиоСКУД СОНДА состоит из собственного ПО, разработанного на основе алгоритмов идентификации по отпечаткам пальцев, которые протестированы в Институте стандартов США и Институте проблем информатики Российской академии наук (ИПИ РАН).
Биометрические IP-терминалы имеют в своем составе оптические сканеры с разрешением до 1000 dpi, что позволяет решать проблему с муляжами.

алгоритмам. Результат всем известен – доминирование на рынке карточных СКУД. За десятилетие произошли серьезные сдвиги не только в скоростных и надежных алгоритмах идентификации, но и в появлении на рынке отечественных биометрических терминалов с повышенным до 1000 dpi разрешением, что позволило сократить время реакции исполнительного механизма (турникет или замок) до 1–1,5 сек., не более. Что уже сравнимо с карточными системами, как по времени прохода, так и по стоимости с учетом затрат на приобретение карт, печати на них логотипов компании, а также компенсации за утерянные пропуска.

Говорить об удобстве использования собственных идентификаторов (пальцев) в настоящее время не приходится. Внедрение сканеров отпечатков пальцев в смартфонах произвело революцию в сознании людей: во-первых, это удобно, во-вторых, это надежно и безопасно.

Для того чтобы БиоСКУД удовлетворяли возросшим требованиям, необходимо выполнение следующих условий.

1. Модульность и интеграция биометрических терминалов с любыми видами карточных СКУД с целью сохранения имеющейся отчетности, интеграции с кадровыми службами, бюро пропусков, бухгалтерии и т.д.

2. Наличие сервера идентификации, в котором хранятся только математические шаблоны сотрудников и их ID-номера. Персональные данные хранятся на сервере карточной СКУД. Тем самым будет соблюден принцип обезличивания персональных данных (ПД), которые можно отнести к 4-ой категории защиты. Это существенно облегчит жизнь операторам ПД и выполнение требований 152 ФЗ.

3. Снижение времени реакции системы через БиоСКУД до параметров карточных систем (не более 1-1,5 секунд независимо от объема базы данных предприятия).

4. Использование бесплатных СУБД, например, PostgreSQL и ОС Linux с открытыми кодами.

Алексей ГИНЦЕ,
PR-директор, ООО «Компания «ААМ Системз»

1. Для начала определимся, что такое биометрический терминал контроля доступа и УРВ (БТКД). Я понимаю под данным определением биометрический считыватель, совмещенный с контроллером СКУД и аппаратным терминалом учета рабочего времени. Считаю, что устройство может быть отнесено к данному классу только в том случае, если оно способно выполнять базовые функции СКУД и УРВ, а также управлять «устройством преграждающим управляемым» (дверь, турникет, шлагбаум и пр.) автономно. Если при этом оно подключается и может управляться в on-line режиме с компьютера, это уже дополнительная приятная опция.

Говоря о трендах, я бы упомянул два. Первый – это смещение функционала в сторону классических терминалов учета рабочего времени, имеющих много аппаратных функций именно УРВ. Функционал СКУД в этом случае не основной, и терминал может вообще не управлять запорным устройством. Второй – когда биометрический считыватель, объединенный с контроллером в одном корпусе, оснащается клавиатурой с выделенными под УРВ функциональными кнопками. В этом случае основная роль обычно принадлежит СКУД.

2. Можно выделить два типа заказчиков. Первый – большое предприятие (отраслевая принадлежность не важна), где установлена крупная сетевая СКУД с выделенным сервером и рядом управляющих компьютеров. Заказчику необходимо на входах и выходах сохранять базовые функции УРВ даже при нарушении связи с компьютерами. В этом случае на внешних точках доступа ставятся мультиформатные терминалы, способные читать как биометрию, так и идентификаторы, используемые на внутренних точках доступа (обычно это не биометрия, а RFID – proximity или smart карты, смартфоны). В этом случае применяют не БТКД, а мультимодальный ТКД, читающий как биометрию, так и карты или смартфоны. Он – только часть крупной интегрированной системы безопасности (ИСБ), включающей не только СКУД, но и обычно еще подсистемы CCTV и ОПС.

Второй случай – офис небольшой компании, магазин, транспортный объект и пр., где ключевая задача – это УРВ. Терминалы БТКД в этом случае также ставятся на входах (или в крупных структурных подразделениях), они часто вообще не управляют дверьми или другими преграждающими устройствами. Их задача – зарегистрировать, когда человек пришел/ушел на работу, когда и с какою целью уходил.

3. Перечислю характерные особенности современных БТКД:

- Возможность функционирования в on-line и off-line режимах.
- Автономное хранение базы данных идентификаторов и событий.
- Наличие клавиатуры и дисплея.
- Наличие функциональных кнопок: приход, уход, обед и пр.
- Подключение к внешним контроллерам СКУД в качестве считывателя.
- Использование разных биометрических признаков (отпечаток пальца, лицо, рисунок вен). Обычно берется один вариант, но можно встретить и мультибиометрические устройства.
- Чтение proximity, smart идентификаторов в дополнение к биометрическим, а также смартфонов.
- Наличие релейных выходов для управления дверью/турникетом/шлагбаумом.

Александр ГОРШКОВ,
директор по развитию компании «Прософт-Биометрикс»

Изначально терминалы контроля доступа создавались под ручное управление сотрудниками охраны. Позже для прохода стали использовать идентификационные карты. Позднее на терминалы стали устанавливать оборудование биометрической идентификации, но решения получались неэстетичные. Современное оборудование для контроля доступа специально разрабатывается с учетом возможности использования биометрических технологий. Это позволяет предложить заказчику наиболее удобное в эксплуатации решение. Скажем, ставить в современный офис оборудование, разработанное для применения на промышленном предприятии, нельзя. Зарубежные производители давно предлагают самые разнообразные по назначению и условиям эксплуатации устройства. Отечественные производители также стали уделять внимание дизайну и эксплуатационным требованиям, предлагая, например, оборудование не только для эксплуатации в экстремальных условиях и на производстве, но и в современных офисных зданиях, коттеджах и многоквартирных домах.

BioSmart (Прософт-Биометрикс)

Биометрическая идентификация по венам ладони на базе линейки устройств BioSmart характеризуется высокой точностью и скоростью распознавания. Вероятность ошибочного предоставления доступа FAR – 0.00008%. Время идентификации 1:1000 – не более двух секунд.**

Спектр возможностей: эксплуатация в нефтегазовом секторе в условиях Крайнего Севера; обеспечение круглосуточного контроля доступа в территориально распределённых организациях (ресторанные сети, ритейл); применение в целях усиленной защиты: на режимных объектах и в финансовых организациях, на промышленных предприятиях и в аэропортах.

Оборудование BioSmart имеет все необходимые сертификаты:

- сертификат соответствия постановлению правительства РФ №969 «Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и правил обязательной сертификации технических средств обеспечения транспортной безопасности»;

- сертификат Научно-исследовательского института медицины труда, подтверждающий безопасность оборудования BioSmart для повседневного использования;

- сертификат электромагнитной совместимости технических средств»;

- сертификат совместимости с системами Astra-Linux, «1С: Предприятие» и др.

Прошло время, когда биометрическим технологиям не доверяли, также прошло и время внедрений на волне восторженной рекламы. Сегодня практически все понимают, что биометрические системы контроля доступа надёжнее традиционных СКУД, и их значительно сложнее обмануть. Но любая биометрическая СКУД потребует дополнительных затрат.

Изменение экономической ситуации в стране и осознанное понимание возможностей биометрической идентификации сформировали новый портрет заказчика. Это человек, который знает, что хочет получить от предлагаемых на рынке решений, какой экономический эффект ожидается и какие функции ему потребуются. Например, контроль доступа в помещение с одновременной проверкой на отсутствие алкогольного опьянения. Или контроль доступа и интеграция с кадровой системой / системой заказа пропусков. Сегодня функционал интеграции с различными кадровыми системами и системами учёта рабочего времени – стандартное дополнение ко многим СКУД.

Появление на рынке новых разработчиков усилило конкуренцию, а это, в свою очередь, приводит к созданию более функциональных биометрических решений, и в то же время более доступных по цене. Появились требования к системам контроля доступа для обеспечения транспортной безопасности, запросы на функционирование в различных климатических условиях. Оборудование для биометрического контроля доступа по рисунку вен ладони применяется на промышленных предприятиях, в нефтегазовом секторе, в ресторанной сети, в сфере ритейла, в финансовых организациях, на режимных объектах и в аэропортах.

Бесконтактный сканер отпечатков пальцев MorphoWave (IDEMIA)

Несмотря на развитие технологий и растущий ассортимент терминалов, для рядового пользователя наиболее понятным методом идентификации все-таки остается дактилоскопия. Компании Morpho (IDEMIA) удалось преодолеть главный минус этого метода – необходимость непосредственного контакта пальца со сканером, и теперь бесконтактный сканер отпечатков пальцев MorphoWave является практическим идеалом современного биометрического терминала. Для идентификации достаточно быстро провести ладонью над терминалом. Сканер считает отпечатки всех пальцев, и если хоть один совпадает с зарегистрированным шаблоном, пропустит посетителя.

Александр ЛЫТКИН,
директор по развитию ООО «СТА»

– В последнее время биометрия набирает все большую популярность. Причем если раньше биометрические терминалы ставились исключительно для ужесточения контроля за посетителями и персоналом, то сегодня наблюдается тенденция к использованию биометрии также для повышения удобства. Так, например, при использовании современных терминалов с распознаванием лиц сотруднику не только не нужно доставать и прикладывать RFID-карту, но и просто останавливаться – система сканирует лица на расстоянии и открывает турникет заранее.

Второй тенденцией, которую мы наблюдаем, является смещение предпочтений в сторону бесконтактных технологий. Это распознавание лиц, сканирование радужной оболочки глаза, бесконтактное сканирование отпечатков пальцев.

Андрей ХРУЛЕВ,
директор по бизнес-развитию направления биометрических систем группы компаний ЦРТ

– До недавнего времени сегмент решений контроля доступа отличался стабильностью в плане использования технологий (магнитные карты, кодовые замки и т. д.), но развитие искусственного интеллекта привело к началу перемен.

Представьте себе пропуск, который нельзя забыть или потерять — это наши уникальные биометрические характеристики (голос, лицо, отпечатки пальцев). Например, биометрические системы распознавания лиц сегодня находят все большее применение, в том числе, в СКУД государственных и коммерческих объектов. В современных бизнес-центрах такая биометрическая система может заменить пропуска и обеспечить мгновенный доступ, что имеет огромное значение при возникновении чрезвычайных ситуаций. В медицинских учреждениях биометрия незаменима для организации доступа в помещения, требующие стерильности: распознавание лиц и радужной оболочки не требуют физического взаимодействия с терминалом. В то же время, бесконтактные терминалы облегчают доступ людям с ограниченными возможностями, да и в целом это более современно и комфортно.

Повсеместное применение биометрических СКУД связано с выбором биометрии все большего числа пользователей, удобством использования и значительным сокращением затрат. Последнее обеспечивается, в частности, возможностью интеграции СКУД на базе распознавания лиц с существующей системой видеонаблюдения. А в сочетании с облачными технологиями экономия будет еще существеннее.

Дальнейшее развитие биометрических СКУД мы видим в повышении эффективности не только самих биометрических технологий, но и технологий антиспуфинга (защиты от взлома), обеспечивающих защиту от атак путем подмены реального пользователя мошенником с помощью поддельного идентификатора. Механизмы защиты будущего должны предвидеть развитие технологий спуфинга и быстро адаптироваться к новым угрозам: чем доступнее становятся современные технологии, облегчающие взлом системы, тем более прогрессивными должны быть алгоритмы защиты. Мы всегда должны быть на шаг впереди, чтобы достичь безопасности и удобства пользователя.

Еще одним трендом можно назвать так называемую «мягкую» биометрию (soft biometrics). Концепция подобных СКУД строится на возможности распознавания по таким признакам, как походка, одежда, наличие или отсутствие бороды, характерных аксессуаров и т.д. Идентификация по дополнительным признакам способна усилить

Биометрическая система распознавания лиц «Визирь» (Группа компаний ЦРТ)

Продукт построен на собственных алгоритмах биометрической идентификации, основанных на нейронных сетях. «Визирь» способен находить и идентифицировать лица, как на фото, так и в видеопотоке в реальном времени, вести структурированную картотеку фотоизображений и сопутствующей информации, осуществлять поиск лиц по этой картотеке.

Система позволяет работать с любыми сторонними фото- и видеоматериалами, может использоваться для решения широкого спектра бизнес-задач: осуществление верификации, контроля доступа, обеспечение общественной и корпоративной безопасности — будь то бизнес-центр, стадион, аэропорт или глобальная система городского масштаба.

Биометрическая система распознавания лиц «Визирь» прошла сертификацию ФСБ РФ для транспортной безопасности. Получение сертификата регламентируется требованиями, отраженными в постановлении правительства № 969 от 26 сентября 2016 года.

Системой «Визирь» уже оснащено 5 аэропортов, 6 железнодорожных вокзалов, более 10 стадионов и ледовых арен. Четыре российских города внедрили отдельные решения ЦРТ для Smart City.

надежность традиционной биометрии в некоторых сценариях, например, в условиях недостаточного освещения.

Внедрение биометрических решений на инфраструктурных объектах России идет полным ходом. Крупнейшие ледовые арены и стадионы используют биометрические системы распознавания лиц, чтобы защищать своих гостей от хулиганов, сделать проход на стадион комфортнее, а местонахождение на нем — безопаснее.

Так, стадион Петровский — первое в мире реальное внедрение биометрии на спортивном объекте. Системы работают в аэропортах и на железнодорожных вокзалах по всей России. При этом важно, что безопасность — базовый, но не единственный сценарий применения технологий распознавания лиц: данные в обезличенной форме можно использовать для улучшения клиентского опыта, например, для оптимизации пассажиропотока на транспорте. На основе биометрии можно создавать дружелюбную городскую среду — будь то проход на стадион, в музей или аэропорт, — среду, с которой человеку легко и приятно взаимодействовать.