



Никита Якубов

Лицевая биометрия в системах контроля и управления доступом и не только

Биометрические методы идентификации человека уже довольно плотно вошли в нашу повседневную жизнь. В статье рассмотрены тенденции развития лицевой биометрии и представлены различные технологии её исполнения. Также описаны основные области её применения и приведены примеры использования, в том числе в России на базе терминала BioSmart Quasar производства отечественной компании «Прософт-Биометрикс».

Биометрические методы идентификации человека уже довольно плотно вошли в нашу повседневную жизнь. Одним из них является технология распознавания лиц. В 2017 году мы стали свидетелями выхода её на массовый рынок в составе iPhone X компании Apple с запатентованной технологией Face ID.

Что такое РАСПОЗНАВАНИЕ ЛИЦ?

Распознавание лиц (Face Recognition) — это один из наиболее перспективных методов биометрической бесконтактной идентификации человека по лицу.

Первые системы распознавания лиц были реализованы как программы для компьютера. В наше время технология

распознавания лиц наиболее часто используется в системах видеонаблюдения, контроля доступа, на разнообразных мобильных и облачных платформах. Журнал Массачусетского технологического института MIT Technology Review включил технологию распознавания лиц в список десяти прорывных технологий 2017 года.

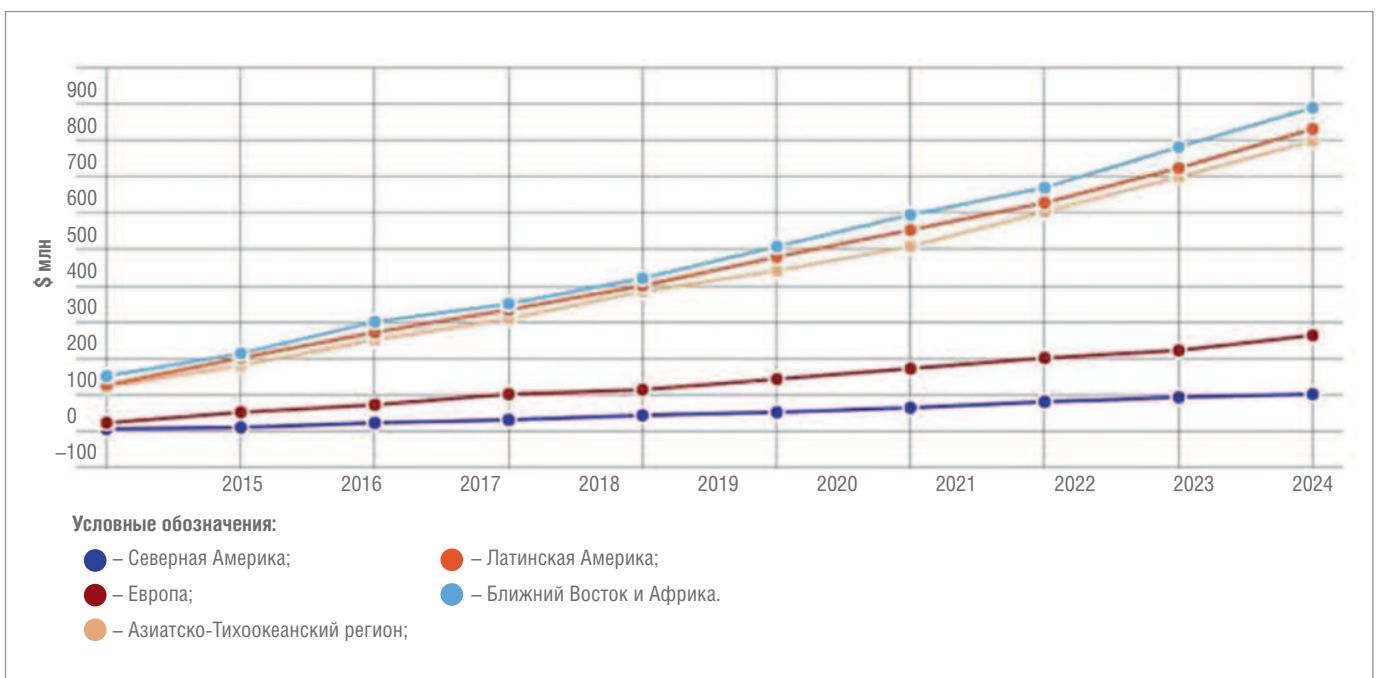


Рис. 1. Годовой доход от технологий распознавания лиц по регионам, 2015–2024 гг.

По оценке Bloomberg, мировой рынок распознавания лиц вырастет с \$4,05 млрд в 2017 году до \$7,76 млрд к 2022 году. На рис. 1 приведены сведения (с прогнозом развития) о годовом доходе от технологий распознавания лиц на мировом рынке по регионам, основанные на данных исследовательской компании Omdia/Tractica.

КАК РАБОТАЕТ СИСТЕМА РАСПОЗНАВАНИЯ ЛИЦ?

В принципе, система распознавания лиц может быть описана как процесс сопоставления лиц, попавших в объектив камеры, с базой данных ранее сохранённых и идентифицированных изображений лиц-эталонов.

Можно выделить три распространённые схемы структурной реализации системы распознавания лиц.

1. Наиболее распространённая схема реализации: IP-камера передаёт видеопоток на сервер, где специализированное программное обеспечение выполняет анализ видеопотока (рис. 2) и сравнение полученных из видеопотока изображений лиц с базой лиц-эталонов.

Недостатки: высокие нагрузки на сеть и стоимость сервера. Даже к самому мощному серверу можно подключить ограниченное количество IP-камер, то есть чем масштабнее система, тем больше требуется серверов.

Преимущество: возможность использовать уже существующую систему видеонаблюдения.

2. На рис. 3 показан случай, когда анализ изображения производится в самой камере, а на сервер передаются обработанные метаданные.

Недостатки: нужны специальные камеры, выбор которых в данный момент не столь широк, как обычных IP-камер, и их стоимость существенно выше. В системах различных производителей будет по-разному решаться вопрос хранения и размера базы данных распознанных лиц-эталонов, а также вопрос взаимодействия ПО камеры и сервера.

Преимущество: подключение практически неограниченного количества камер к одному серверу.

3. В отличие от первых двух схем, где используются IP-камеры, в данном случае камера встроена в устройство контроля доступа (рис. 4), которое кроме распознавания лица выполняет функции управления доступом через турникет или электромеханиче-

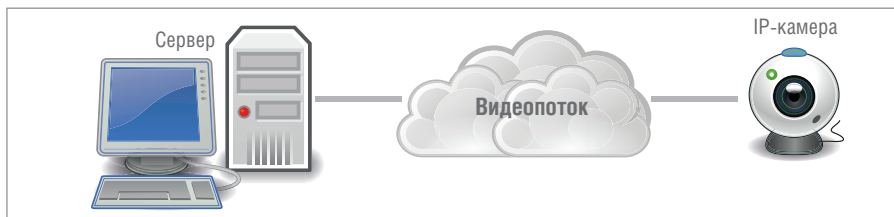


Рис. 2. Вариант анализа видеопотока на сервере

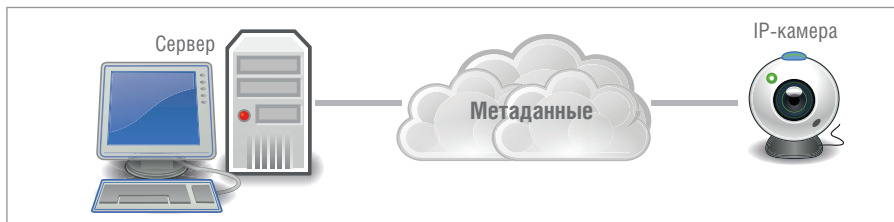


Рис. 3. Вариант анализа видеопотока в IP-камере



Рис. 4. Вариант анализа видеопотока на устройстве контроля доступа

ский замок, установленный на двери. База данных лиц-эталонов хранится на устройстве и, как правило, уже не в виде фотоизображений. Само же распознавание происходит непосредственно на устройстве.

Недостатки: как правило, все такие устройства выпускаются для использования в помещениях.

Преимущество: низкая стоимость системы по сравнению с системами видеонаблюдения, используемыми для распознавания лиц.

В любом случае успех реализации проектов по распознаванию лиц зависит от трёх важных факторов:

- качества и быстродействия алгоритма распознавания лиц;
- качества и полноты базы данных распознанных лиц (эталонов);
- быстродействия устройства.

ТЕХНОЛОГИЯ РАСПОЗНАВАНИЯ ЛИЦ

Как правило, система состоит из камеры видеонаблюдения и программного обеспечения, которое выполняет анализ изображений.

Программное обеспечение распознавания лиц основано на обработке изображений и вычислениях сложных математических алгоритмов, для которых требуется более мощный сервер, чем для обычных систем видеонаблюдения.

2D-распознавание лиц

В основе технологии 2D — двухмерного распознавания лиц — лежат плоские двухмерные изображения. Алгоритмы распознавания лиц используют антропометрические параметры лица, графы — модели лиц или эластичные 2D-модели лиц, а также изображения с лицами, представленные некоторым набором физических или математических признаков.

Распознавание 2D-изображений — одна из наиболее востребованных технологий на данный момент, так как основные базы данных идентифицированных лиц, накопленные в мире, содержат именно двухмерные изображения. И основное оборудование, уже установленное по всему миру, тоже ориентировано на технологию 2D. Именно поэтому основной спрос приходится на 2D-системы распознавания лиц.

Преимущества: наличие готовых баз данных лиц-эталонов и готовой инфраструктуры является огромным преимуществом 2D-распознавания лиц. Максимальный спрос придёт именно на этот сегмент, и он будет стимулировать разработчиков совершенствовать технологии.

Недостатки: более высокие коэффициенты ошибок FAR и FRR по сравнению с 3D-распознаванием лиц. FAR (False Acceptance Rate) и FRR (False Rejection Rate) характеризуют соответ-

Таблица 1

Сравнение эффективности 2D- и 3D-распознавания лиц

Метод биометрической идентификации	Коэффициент ложного пропуска, FAR	Коэффициент ложного отказа, FRR
Распознавание лиц 2D	0,1%	2,5%
Распознавание лиц 3D	0,0005%	0,1%

ственно вероятность ложного совпадения биометрических характеристик двух людей и вероятность отказа в доступе человеку, имеющему допуск (табл. 1).

3D-распознавание лиц

3D-распознавание лиц (Three-Dimensional Face Recognition) проводится, как правило, по реконструированным трёхмерным образам. Технология 3D-распознавания лиц имеет более высокие качественные характеристики, хотя, конечно, и она не является идеальной.

Существует несколько разнообразных технологий 3D-сканирования. Это могут быть лазерные сканеры с оценкой дальности от сканера до элементов поверхности объекта, специальные сканеры со структурированной подсветкой поверхности объекта и математической обработкой изгибов полос, либо это могут быть сканеры, обрабатывающие фотogramметрическим методом синхронные стереопары изображений лиц.

Одним из наиболее исследованных потребителями и экспертами 3D-сканеров является знаменитый Face ID компании Apple. Опыт использования Face ID крайне интересен и показателен, потому что, по сути, это единственное устройство с технологией 3D-распознавания лиц, выпущенное на массовый рынок.

Преимущества: большая точность и меньшее количество ошибок, пока недостижимое для 2D-систем распознавания лиц (табл. 1).

Недостатки:

- 3D-распознавание лиц требует специальных камер для сканирования, которые в несколько раз дороже обычных камер видеонаблюдения, используемых в 2D-распознавании;
- отсутствие готовых баз данных идентифицированных лиц в отличие от 2D-распознавания;
- распознавание близнецов остаётся сложной задачей для алгоритмов распознавания лиц. В среднем в мире рождается 13,1 близнецов на 1000 новорождённых, и эта цифра сильно колеблется в зависимости от географического региона.

ОБЛАСТИ ПРИМЕНЕНИЯ ЛИЦЕВОЙ БИОМЕТРИИ

Специфика применения технологии распознавания лиц (рис. 5) отличается разной критичностью к ошибкам в зависимости от сферы применения.

Системы контроля доступа

Одно из лучших применений систем распознавания лиц на данный момент – системы контроля доступа. Во-первых, сотрудник сам заинтересован в предо-

ставлении ему доступа и не будет сознательно саботировать работу системы распознавания лиц. Во-вторых, контролируются все внешние факторы, влияющие на качество распознавания: освещение, фон, схема движения сотрудников. Используя всё это, можно создать идеальные условия решения поставленной задачи.

Учёт рабочего времени

Ещё недавно учёт рабочего времени без использования преграждающих устройств был недостижимой мечтой. Сегодня это реальность. Учёт рабочего времени – это, конечно, одна из функций системы контроля доступа, но он может вестись и отдельно, только с помощью системы распознавания лиц.

Одно из основных преимуществ использования систем распознавания лиц для учёта отработанного времени в отличие от биометрии по отпечатку пальца, например, – это отсутствие требований к чистоте лица, в пределах разумного, конечно. Также преимуществами учёта рабочего времени с помощью системы распознавания лиц будут отсутствие преграждающих устройств, что повышает комфортность, а также возможность использовать учёт рабочего времени скрытно, без информирования сотрудников.

Распознавание лиц для целей учёта рабочего времени может быть реализовано в двух вариантах:

- сервер + программное обеспечение + хорошие IP-камеры. Это довольно дорогой вариант, но зато учёт рабочего времени в таком случае может вестись без информирования сотрудников;
- специализированные терминалы – это тот вариант, когда сотруднику нужно подойти к терминалу, тем самым выполнив процедуру идентификации. Это работает, только если объявили о том, что любому, кто не отметится в устройстве распознавания лиц, рабочий день засчитан не будет. Такая простая административная мера сокращает количество ошибок FAR и FRR до абсолютного нуля.

Распознавание лиц в транспорте

В транспорте распознавание лиц может применяться для решения нескольких задач:

- подсчёт количества пассажиров, использующих общественный транспорт;

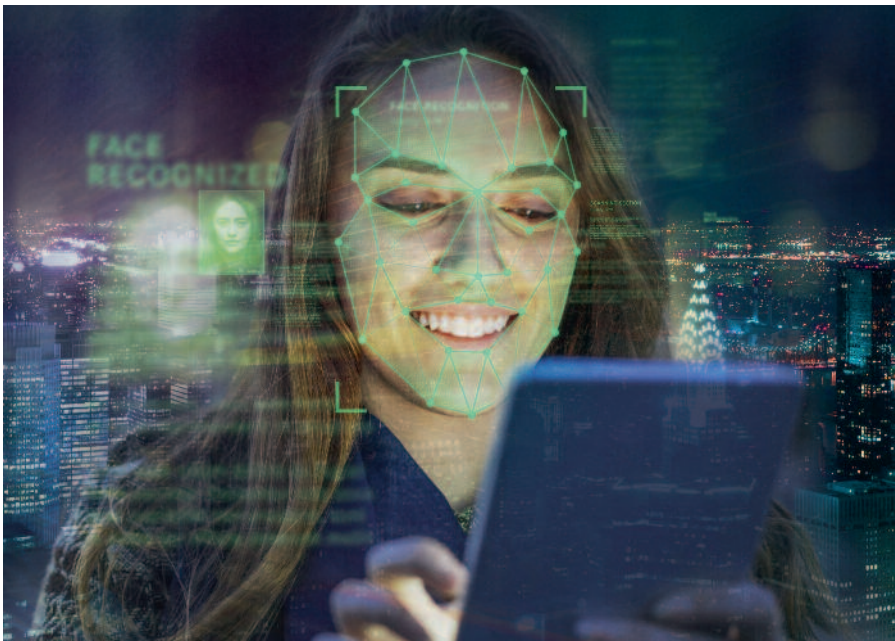


Иллюстрация с сайта rplenskyface.com

Рис. 5. Технология распознавания лиц

- поиск преступников, находящихся в розыске;
- поиск пропавших людей;
- получение демографической информации для лучшего обслуживания.

Данные о количестве пассажиров, поступающие в режиме онлайн, помогут быстрее, более гибко и эффективно управлять сетями общественного городского транспорта. Также подсчёт количества пассажиров при сопоставлении этих данных с количеством оплат позволит фиксировать нарушения правил оплаты проезда.

Распознавание лиц для целей оплаты проезда может на данный момент вестись в режиме верификации и позволит избежать несанкционированного использования многоразовых или персонализированных проездных билетов.

Использование распознанного лица как единственного идентификатора пассажира для автоматизированной оплаты проезда на данном уровне развития технологий представляется возможным только в небольших корпоративных транспортных сетях и никак не подойдёт для городского общественного транспорта.

Маркетинговые задачи

От задач безопасности переходим к задачам маркетинга. Возрастной и гендерный состав посетителей — это бесценная информация. Не нужно быть великим маркетологом, чтобы понимать, что разный возрастной и гендерный состав покупателей требует различной маркетинговой, PR, рекламной и других стратегий, связанных со взаимодействием с клиентами.

Важной задачей для маркетинга, которую можно решить с помощью системы распознавания лиц, является подсчёт уникальных посетителей. Ранее эту классическую задачу всегда решали с помощью инфракрасных или лазерных датчиков, которые просто показывают количество пересечений виртуальной линии. Например, тележка будет давать отдельное пересечение, как и частые перемещения охранников в той же зоне. Все эти погрешности могут сделать данные практически полностью бесполезными.

Многие сетевые магазины, кинотеатры и другие предприятия, обслуживающие большой поток людей, уже тестируют и внедряют системы распознавания лиц для решения описанных задач. Подобные системы также помогают им в выявлении VIP-персон и нежелатель-

ных лиц, при обнаружении которых соответствующему персоналу мгновенно приходят необходимые уведомления. В вопросах выявления мошенников и снижения воровства тоже могут помочь системы распознавания лиц.

Платёжные системы

Ещё недавно использование технологии распознавания лиц в целях верификации платёжной транзакции и в голову никому не могло прийти: слишком ненадёжной, казалось, была технология. Но ещё в 2017 году в Китае компания Ant Financial запустила сервис «улыбка для оплаты» в Ханчжоу (там находится штаб-квартира), где он тестируется совместно с KFC. В данном примере процесс оплаты не требует смартфона, поскольку предполагается, что клиент уже зарегистрировался в приложении Alipay и активировал функцию распознавания лиц. 3D-камера, расположенная в терминале, идентифицирует плательщика, а для дополнительной безопасности есть опция проверки номера телефона [1].

Что касается России, то с внедрением единой биометрической системы (ЕБС) некоторые банки стали предлагать дистанционное предоставление банковских услуг (денежные переводы, кредиты и т.д.) с подтверждением с мобильного телефона связки лица и голоса. Всё, что требуется для использования данной возможности, — это однажды предоставить в отделение банка эталон изображения лица и голоса, сфотографировавшись и проговорив комбинацию цифр. Далее нужно лишь взглянуть во фронтальную камеру телефона и проговорить комбинацию цифр, указанную на экране, для получения той или иной услуги.

Помимо использования телефона для дистанционного предоставления банковских услуг, некоторые кафе, кофейни и прочие предприятия общественного питания используют лицевые биометрические терминалы для оплаты покупок. Один из таких примеров совместно реализовали компании BioSmart и Ростелеком при поддержке банка «Русский Стандарт». Они внедрили сервис оплаты покупок с использованием технологии идентификации по лицу в одной из кофеен сети Coffee Bean.

Совершать биометрические платежи граждане могут после регистрации своих биометрических данных в ЕБС по описанному сценарию. Для того чтобы



Рис. 6. Терминал BioSmart Quasar

совершать биометрические финансовые операции, необходимо привязать платёжную карту к своему цифровому образу, который находится в ЕБС. Сразу после этого можно совершать оплату по биометрии лица.

BioSmart Quasar

Внедрённый биометрический терминал BioSmart Quasar — это новый усовершенствованный прибор для идентификации по лицу.

Терминал BioSmart Quasar (рис. 6) имеет аппаратный модуль стереокамеры с адаптивной подсветкой, которая позволяет с высокой точностью работать даже в условиях недостаточной освещённости. Встроенное ПО предполагает создание гибких сценариев управления доступом.

Устройство имеет широкий набор интерфейсов для быстрой интеграции в сторонние системы контроля и управления доступом. Благодаря удобной конструкции терминал легко установить на стену или на турникет.

Терминал обладает 10-дюймовым сенсорным экраном и мультимедийным считывателем RFID-карт для организации двухфакторной аутентификации. Каждому пользователю могут быть назначены код карты, QR-код, до 10 шаблонов лица и фотография. Подробные характеристики BioSmart Quasar приведены в табл. 2, [2].

Вместо заключения

У технологии распознавания лиц всегда были, есть и будут свои поклонни-

Таблица 2

Характеристики терминала BioSmart Quasar

Процессор	ARM, 6 ядер
RAM	2 Гб
Интерфейсы	Wi-Fi, Bluetooth, Ethernet
Видео	2 камеры RGB + IR, 1,3 Мпк, разрешение каждой камеры 1280 × 960
Считыватель карт	Em-marlin, HID, Mifare Classic, Mifare DESFire, iClass SE
Подсветка	Светодиодная + инфракрасная
Питание	PoE 802.3at 4 класс, 25 Вт
Реле для управления замком	«Сухой» контакт
Порты ввода-вывода	3/3
Интерфейс RS-485	Для подключения дополнительных считывателей
Время идентификации	Не более 1,5 с
Диапазон рабочих температур	0...+50°C
Операционная система	Linux, версия ядра 4.4
Максимальное количество пользователей	100 000
Максимальное количество шаблонов лиц	1 000 000
Максимальное количество хранимых событий	10 000 000
Максимальное количество хранимых событий с фото	100 000

ки и противники. Первые будут совершенствовать алгоритмы и делиться вдохновенными отчётами со всё большим числом девяток после запятой в показателях точности, а вторые, напротив, будут писать разоблачительные статьи о неэффективности подобных систем, даже толком не разобравшись в сути вопроса.

Например, американский союз защиты гражданских свобод (ACLU) решил «уничтожить» Amazon, продемонстрировав «чудовищную» неэффективность

их системы распознавания лиц. Фотографии 535 американских конгрессменов сравнивались с базой из 25 000 фотографий ранее задержанных лиц. Несмотря на заранее известное отсутствие парламентариев на 25 000 фотографий, технология идентифицировала 28 конгрессменов как преступников. На первый взгляд, действительно очевидна неэффективность системы. А теперь давайте посчитаем количество сравнений, которые должна была произвести система. Для этого мы 535 фотографий

конгрессменов умножим на 25 000 фотографий, которые содержались в базе данных, и получим 1 337 500. Из 1 337 500 сравнений 28 оказались ошибочными. То есть корректными оказались 1 337 472. Теперь переведём в проценты: 1 337 472 разделим на 1 337 500 и получим эффективность системы 99,997%.

Для контраста можно привести другой пример. В 2014 году журнал PLOS ONE опубликовал исследование, которое было проведено среди офицеров Австралийской паспортной службы. Смысл исследования состоял в определении точности идентификации предъявителя паспорта по фото в паспорте. В результате специально подготовленные офицеры, имевшие опыт работы по идентификации, в среднем пропускают один из семи паспортов (14% случаев), не принадлежащих предъявителю, то есть корректными оказались лишь 86% случаев. Можете сделать выводы. ●

ЛИТЕРАТУРА

1. Технология распознавания лиц от «А» до «Я» [Электронный ресурс] // Режим доступа : <https://securityrussia.com/blog/face-recognition.html>.
2. Терминал BioSmart Quasar [Электронный ресурс] // Режим доступа : <https://www.biosmart.ru/product/biosmart-quasar>.

**Автор – сотрудник
фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru**

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

«РЕД СОФТ» и «ФАСТВЕЛ» развивают технологическое партнёрство

Российские разработчики «РЕД СОФТ» и «ФАСТВЕЛ» протестировали на совместимость свои продукты. Результаты испытаний подтвердили корректность работы операционной системы РЕД ОС производства «РЕД СОФТ» и процессорного модуля Fastwel CPC518 производства «ФАСТВЕЛ». По итогам был подписан двусторонний сертификат.

РЕД ОС – многопользовательская многозадачная операционная система общего назначения для серверов и рабочих станций, представляющая универсальную среду для использования прикладного программного обеспечения. Продукт обладает сертификатом ФСТЭК России (№ 4060 от 12.01.2019), что подтверждает соответствие требованиям информационной безопасности и допускает его применение в государственных информационных системах. РЕД ОС зарегистрирована в Едином реестре



российских программ для ЭВМ и баз данных Минкомсвязи России (№ 3751).

Процессорный модуль CPC518 выполнен в форм-факторе CompactPCI Serial 3U. Он построен на базе ЦП семейства Intel Xeon D-15xx, Pentium D-15xx с напаянными оперативной памятью (16–32 Гб) и SSD (от 32 Гб). Модуль обеспечивает работу в диапазоне температур –40...+70° С (в исполнении с конвекционным отводом тепла) или –50...+85° С (в исполнении с кондуктивным отводом тепла). Основной сферой применения CPC518 являются работающие в жёстких условиях бортовые и стационарные компьютерные вычислительные системы, в которых

необходимы многоядерные x86-совместимые вычислители с высокой производительностью.

– Расширяя список совместимых с РЕД ОС российских продуктов, мы вносим вклад в технологическую независимость страны. Совместно с коллегами из «ФАСТВЕЛ» предлагаем отечественное решение, направленное на обеспечение безопасности в гетерогенных системах, – комментирует Рустам Рустамов, заместитель генерального директора «РЕД СОФТ».

– «ФАСТВЕЛ» продолжает курс на разработку импортозамещающих вычислительных систем для отечественных пользователей. В этой связи сотрудничество с производителями российских операционных систем, в частности с компанией «РЕД СОФТ», является важным шагом на пути к созданию полноценных программно-аппаратных платформ, способных составить достойную конкуренцию зарубежным аналогам, – отмечает бренд-менеджер «ФАСТВЕЛ» Николай Сергиенко. ●



УНИВЕРСАЛЬНЫЕ БИОМЕТРИЧЕСКИЕ КОМПЛЕКСЫ АВТОМАТИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Для объектов с различными требованиями к системам безопасности

- Уникальные комплексные решения с применением широкого спектра передовых биоидентификационных технологий цифрового будущего
- Полная автоматизация процедур доступа, включая автоматизацию существующих бюро пропусков
- Защита специализированных помещений и входных групп зданий
- Готовность к работе в рамках последних решений правительства в области цифровизации идентификационных документов
- Изделия соответствуют государственным стандартам в области защиты персональных данных
- Разработаны и производятся в России
- Изготовлены с применением надежных промышленных комплектующих
- Реализация требуемых сценариев прохода с любой комбинацией механизмов идентификации, включая различные бесконтактные методы
- Полностью готовы к интеграции в инфраструктуру пунктов контроля
- Оптимальная совокупная стоимость владения

