Что делает турникеты умными?

Дмитрий Швецов

Зачастую турникеты становятся одним из основных компонентов любой комплексной стратегии физической безопасности. Современные технологии сыграли большую роль в продвижении турникетов с момента их скромного появления в начале XX века до многофункционального компонента безопасности в повседневной жизни. Чтобы понимать, как будут развиваться в ближайшем будущем технологии преграждающих устройств и физической безопасности, имеет смысл проследить эволюцию самих турникетов.

Первоначальная цель создания турникетов относится к сельскохозяйственной отрасли, где существовала потребность в том, чтобы люди могли переходить с поля на поле, одновременно удерживая скот в загоне. В начале века основатель одной из первых сетей супермаркетов впервые установил турникеты, чтобы контролировать толпы людей, жаждущих посетить первый в мире супермаркет.

С этого момента турникеты быстро завоевали популярность как метод ограничения и контроля входа и выхода из различных объектов, таких как вестибюли офисов, стадионы, парки развлечений, аэропорты, жилые дома и промышленные предприятия. Старые модели – вращающиеся турникеты в виде штатива и штанг – широко использовались в метро и на спортивных стадионах, но в настоящее время постепенно выводятся из употребления или серьёзно модифицируются, поскольку в них нет датчиков или каких-либо других средств безопасности. Помимо всего прочего, они оказались очень опасными для детей.

Дальнейшее развитие технологий турникетов шагнуло гораздо дальше задач контроля толпы в сторону обеспечения широкого круга сервисов и комплексной безопасности. Турникеты стали намного безопаснее и интеллектуальнее, отчасти благодаря использованию бесконтактных технологий и миниатюризации вычислительных устройств для высокоточного анализа того, что происходит в створе турникетного прохода. Появилась возможность встраивать в них другие интеллектуальные инструменты, такие как карты доступа, биометрические сканеры и программное обеспечение для распознавания лиц, рисунка вен ладоней радужной оболочки глаз. Но что означает этот встроенный интеллект для реализации задач контроля входа? По сути, эти задачи, от самых простых до очень сложных, предназначены для одной лишь цели: разрешить доступ людям, имеющим право доступа и эффективно препятствовать проходу тех, у кого этих прав нет. Встроенная в турникеты интеллектуальная система позволяет пользователям применять комплексный подход к системе контроля доступа, а не ограничиваться решением одной или двух ключевых функций. Рассмотрим некоторые предложения интеллектуальных технологий, которые действительно делают турникеты «умными».

Инфракрасные барьеры

Благодаря каскадному использованию инфракрасных датчиков, пересекающих проходы, турникеты самостоятельно могут определять, когда кто-то пересёк одну пару или группу лучей. В самом начале применения ИК-барьеров обнаружение пересечения луча было единственной информацией, с которой должен был работать встраиваемый вычислитель, чтобы определить, проходит ли кто-то через турникет и в каком направлении. Устаревшие технологические системы часто не могли точно «понять», что конкретно происходит внутри турникета, и ошибочно закрывали створки прямо на толкаемые или тянущиеся сумки, тележки или детские коляски. Они также могли обрабатывать проход только одного авторизованного пользователя, проходящего через турникет единовременно, поэтому другим посетителям приходилось ждать, пока человек перед ними полностью не пройдёт.

Интересно отметить, что некоторые из этих старых турникетов с технологией пересечения ИК-лучей всё ещё находятся на сегодня рынке, хотя некоторые из них изменили конфигурацию и дизайн, чтобы скрыть устаревшие технологии. Их легко определить по низкой пропускной способности (менее 30 человек в минуту) и по предупреждениям об использовании этих турникетов детьми.

Нейронные сети

Интеллектуальные турникеты могут иметь до девяти микропроцессоров на каждом турникетном проходе, чтобы обеспечить работу с нейронной сетью и точно моделировать каждый объект, оказавшийся в поле зрения. Например, сумки теперь уже рассматриваются как часть авторизованного пользователя, и, если второй авторизованный пользователь появляется в створе турникетного прохода, они моделируются отдельно, без ложных срабатываний и дополнительного закрытия створок. Этот уровень интеллекта также повышает эффективность обнаружения багажа и

его габаритов в турникетах, установленных в аэропортах.

Аварийный режим работы

В случае срабатывания пожарной сигнализации каждый современный турникет должен открываться в направлении выхода, чтобы люди могли покинуть аварийный объект. Для безопасного прохода необходимо учитывать аварийные ситуации, когда людям, находящимся на безопасной стороне турникетов, необходимо выйти. В этом случае они не должны подавать сигналы тревоги и не должны возвращаться к нормальной работе до тех пор, пока не будет отключена пожарная сигнализация.

Но есть ещё одна ситуация, которую не учитывают некоторые производители: аварийный выход в случае пожарной опасности при несработавшей вследствие человеческого фактора пожарной сигнализации. Люди с защищённой стороны турникета должны иметь возможность покинуть его без дополнительной авторизации. Интеллектуальные турникеты безопасности могут отключать блокирующие устройства и позволять пользователям открывать створки вручную, как только они оказались на безопасной стороне турникета. Сигнал тревоги должен срабатывать, когда неавторизованные пользователи прорываются через створки турникета, но в случае возникновения опасности интеллектуальный турникет позволяет открыть створки для обратного прохода. Эта функция становится обязательной и всё более востребованной в строительных и противопожарных нормах по всей стране.

Биометрия

Технология биометрической безопасности продолжает стремительно развиваться, и многие учреждения стремятся улучшить качество безопасного взаимодействия с пользователем без необходимости физического контакта и прикосновения к чему-либо, а также без дополнительного предъявления учётных данных. В этой связи турникеты всё чаще оснащают биометрическими сканерами с самыми передовыми технологиями бесконтактной идентификации от разных поставщиков, которые могут интегрироваться с широким спектром биометрических продуктов, включая распознавание лиц, сосудистого рисунка вен ладоней и радужной оболочки глаз. Зачастую две и более биометрические модальности были интегрированы в этих решениях, и практически все из них полностью бесконтактные.

IP-связь

Эффективность умных турникетов зависит от текущих настроек встраиваемого программного обеспечения и его актуальности для выполнения текущих задач. В турникетах с IP-поддержкой актуальность программного обеспечения и критически важные настройки можно загружать в удалённом режиме, а не обновлять их физически непосредственно на устройстве. Возможность обновления встраиваемого программного обеспечения и его настроек в режиме реального времени обеспечивает максимальное непрерывное время безотказной работы и высокую производительность при соблюдении требований политик безопасности. Поддержка криптографической защиты при IP-связи с вычислительными средствами турникетов, будь то с выделенного устройства дистанционного управления, из веб-браузера или с использованием доступных последовательностей команд CGI/XML, может позволить службам безопасности контролировать работу проходов в автоматическом режиме в нерабочее или вечернее время для повышения безопасности объектов, когда не требуется большого количества сотрудников безопасности.

Умные биометрические турникеты сегодня

Рассмотрим, как в умные турникеты интегрируются биометрические технологии. До сего времени было и есть много опасений, связанных с конфиденциальностью использования биометрии, а также общее чувство страха перед самой технологией. Современные государственные и частные предприятия очень часто включают биометрический контроль доступа в свою стратегию безопасности. В этой связи очень важно учитывать как проблемы, так и возможности широкого применения биометрии на предприятиях.

Начнем с фактора страха. Зачастую мы наблюдаем опасения по поводу воздействия лазера ближнего инфракрасного диапазона на зрение и некоторые опасения, что нахождение в непосредственной близости от любых биометрических сканеров может испускать какую-то форму электромагнитного излучения, что совершенно не соответствует действительности. А ещё есть технология, раздражающая многих: «проверка на живучесть», используемая некоторыми старыми сканерами радужной оболочки глаза. Эти сканеры светят в глаз, чтобы дополнительно увидеть, сужается ли зрачок. Свет часто пугает людей, и они отводят взгляд. Это приводит к тому, что сканер теряет объект распознавания, и совпадение биометрических показателей не происходит. Повторная попытка сканирования так же неприятна для пользователей этой системы.

Серьёзной проблемой конфиденциальности для многих является то, что, если их биометрические данные собираются для одной цели, то в дальнейшем они могут быть использованы для других целей. Например, возможно, биометрический контроль доступа используется для защиты доступа к рабочему месту. Некоторые опасаются, что эти данные могут быть использованы против них позже для чего-то, совершенно не связанного с этим, если правоохранительные органы получат к ним доступ. Хотелось бы развеять опасения именно по поводу этой проблемы, потому что биометрические шаблоны нельзя использовать для воссоздания изображения лица или рисунка вен ладоней. А если в вашем учреждении используются смарт-карты для контроля доступа, биометрические данные обычно хранятся на карте, и никто не может получить к ним доступ.

Что касается системы видеонаблюдения и всех камер, записывающих повседневную жизнь людей, а затем пытающихся сопоставить их лица с лицами подозреваемых в терроризме или преступлениях, то дело не в технологии, а в том, как она используется.

В настоящее время наиболее широко применяется биометрия для более удобного контроля доступа, которая включает отпечатки пальцев, рисунок вен ладоней, распознавание лиц, сканирование радужной оболочки глаз. В течение последних нескольких лет компании-лидеры в области биометрии разработали надёжные методы и технологии биометрической аутентификации в ответ на вызовы современного рынка к защите биометрических данных и критической инфраструктуры предприятий.

Рассмотрим применение биометрии и причины, по которым она необходима в различных ситуациях, которые часто остаются за рамками биометрических дискуссий. Использование биометрических данных для целей уголов-

ного расследования или идентификации террористов обычно попадает в заголовки газет с хорошо задокументированными заявлениями о вторжении в «частную жизнь» с помощью любой камеры, участвующей в поимке преступников. Однако использование тех же биометрических устройств для простого контроля доступа в офисах гораздо менее актуально и редко упоминаются в СМИ.

Давайте сосредоточимся на некоторых из этих различий в способах применения биометрии.

Биометрия для контроля доступа

Системы контроля доступа для лиц, входящих в охраняемый объект, используют биометрические данные только для проверки личности. В этих случаях лицо, подходящее к входным турникетам, воротам или дверным проёмам, должно предоставить доказательство того, что оно является тем, за кого себя выдаёт, чтобы сотрудник мог войти в здание и приступить к работе. Предварительно сотрудник был зарегистрирован в системе управления доступом объекта с рядом атрибутов, таких как ID сотрудника, имя, отдел и права доступа. Такие атрибуты могут включать разрешение на доступ в помещения, в которые они могут входить, утверждённые графики доступа и многое другое. Эти основные атрибуты могут быть связаны с сохранённым биометрическим шаблоном лица и/или рисунка вен ладоней, а также с документом, удостоверяющим личность. Обратите внимание, что биометрические шаблоны не являются сохранёнными изображениями фактических биометрических данных.

В зависимости от учреждения биометрические шаблоны, собранные во время регистрации, могут храниться в базе данных для последующего обработки и удалённого доступа. Они также могут храниться на специальной идентификационной карте, называемой смарт-картой. Смарт-карты остаются у сотрудника, и хранящиеся на нем биометрические шаблоны сопоставляются с ним, когда он предъявляет свою карту, чтобы подтвердить, что он является лицом, которому была выдана карта.

Шаблоны управления доступом создаются во время регистрации компьютером, математически генерирующим ряд «единиц» и «нулей» на основе сканирования фактических биометрических данных, т.е. лица или рисунка вен ладоней. Фактические изображения биометрического элемента никогда и нигде не сохраняются во время этого процесса без явного ведома и согласия сотрудника. С этого момента все последующие «совпадения» с личностью этого человека производятся мгновенно, когда сотрудник подходит к биометрическому сканеру. В этот момент сканер создаёт новый математический шаблон «единицы» и «нули» их «живого лица» или вен ладоней, которые используются для сопоставления с исходными биометрическими шаблонами.

Чтобы было ясно, биометрические шаблоны, созданные для контроля доступа, нельзя использовать для воссоздания фактического рисунка вен ладоней или изображения лица для сравнения с криминальными базами данных. Если обязательным условием приёма на работу не является обязательная проверка биографических данных, полные изображения отпечатков пальцев фактически не собираются во время регистрации для целей контроля доступа. Для проверки биометрических данных работодатель в соответствии с 152-ФЗ обязан уведомить потенциальных сотрудников об этом требовании до сбора необходимых изображений, а потенциальный сотрудник имеет право согласиться или отказаться.

Биометрия для общей проверки личности

Ещё одной растущей областью использования биометрии является транспортная отрасль, особенно в аэропортах. Конкретные требования варьируются от страны к стране, но, независимо от того, где это делается, пассажир должен подтвердить свою личность, подтвердить, что его идентификационные данные действительны и принадлежат ему, и что его имя совпадает с именем в посадочном талоне, прежде чем он сможет сесть на борт самолета. Всё чаще эти перекрёстные проверки осуществляются с помощью биометрии.

Большое количество пилотных проектов с использованием биометрии устанавливается в аэропортах по всему миру. Одно из крупнейших испытаний проводится в аэропорту Чанги в Сингапуре, где в одном терминале пассажир может пройти от тротуара до своего места в самолёте, даже не разговаривая с реальным живым человеком.

Ключевое различие между этими общими вариантами использования для проверки личности и ситуациями контроля доступа заключается в том, что пассажиры сравнивают свои биометрические данные с шаблоном, ранее собранным государственным учреждением и хранящимся в электронном паспорте, карте Trusted Traveller или расширенных водительских правах, имеющихся у пассажиров. По функциям они аналогичны смарт-картам контроля доступа, упомянутым ранее, но в этом случае аэропорты или авиакомпании не контролируют их выпуск.

В некоторых пилотных проектах фотографии лица «неэлектронных» удостоверений личности или паспортов сканируются и сравниваются с «живым» лицом пассажира для должной степени совпадения. В то же время проверяются и атрибуты самого документа, чтобы убедиться, что они действительны, что срок их действия не истёк и что имя на документе совпадает с именем на посадочном талоне. Несмотря на проблемы с качеством изображения во многих из этих документов, решение такого типа будет востребовано в течение некоторого времени, пока все выданные государством документы, удостоверяющие личность, не смогут хранить биометрические шаблоны в электронном виде. И сопоставление фотографии с лицом живого человека — это именно то, что делается, когда авиакомпания или сотрудник транспортной безопасности проверяет документ, а затем смотрит на человека. Однако оказалось, что электронное сканирование получалось примерно на 20% точнее, чем это делали сотрудники транспортной безопасности, которые были вовлечены в пилотные проекты.

Вариант этого подхода к проверке личности используется во многих аэропортах для таможенного и пограничного контроля. Биометрический шаблон лица, хранящийся в электронном паспорте человека, сравнивается с его живым лицом для подтверждения его личности. Такой подход может значительно сократить задержки при пересечении границы, позволяя сотрудникам паспортного контроля сосредоточить своё внимание на пассажирах, которые нуждаются в ручной обработке, позволяя другим быстро пройти через автоматизированные системы паспортного контроля.

В качестве примера рассмотрим ряд технологий, интегрированных в умные турникеты для предотвращения несанкционированного доступа на территорию предприятия. Одним из таких

способов является «приклеивание» сотрудников. Речь идет о попытке неавторизованного лица получить доступ в здание, следуя за авторизованным лицом через турникет. В одном из умных турникетов интегрированы технологии ИК-барьеров и искусственный интеллект на базе встроенной системы видеоаналитики. Эскизное изображение умного турникета с этими технологиями представлена на рис. 1.

В турникетах традиционно применяют системы детекции с активными ИК-датчиками, состоящими из двух частей: излучатель – источник инфракрасного излучения и приёмник – устройство, улавливающее это излучение и преобразующее его в электрический сигнал. Когда в створе турникетного прохода в зоне действия датчиков нет посетителя, ИК-лучи передатчика свободно достигают приёмника и устройство находится в дежурном режиме. Но как только лучи пересекает человек, связь моментально нарушается, и приёмник отправляет на встроенный контроллер турникета соответствующий сигнал. Для интеллектуального турникета, представленного на рис. 1, применена комбинированная система, состоящая из набора диффузных датчиков приближения и ИК-барьеров. В системе используется три ИК-барьера, которые формируют соответствующие сигналы при одновременном прерывании двух и более соседних лучей из имеющихся восьми, если время прерывания превышает заданное значение (40–80 мс) запускается алгоритм детекции посетителя и активируется подсистема видеоаналитики. К особенностям ИК-барьеров можно отнести, что они формируют очень узкую зону обнаружения движения, и её можно регулировать по горизонтали и вертикали для более чёткого определения количества посетителей и предметов, появляющихся в створе турникета. Помимо комплексной системы ИК-датчиков и барьеров, интеллектуальный турникет имеет встроенную биометрическую систему с искусственным интеллектом с элементами нейросетевой аналитики. При построении подобных интеллектуальных систем с биометрией широко применяются нейросетевые методы распознавания лица. Нейронная сеть состоит из элементов, называемых формальными нейронами, каждый из которых элементарен по структуре и связан с другими нейронами. Каждый нейрон преобразует совокупность сигналов, поступающих к нему на вход, в выходной сигнал. Именно связи между нейронами, кодируемые весовыми коэффициентами, играют ключевую роль.

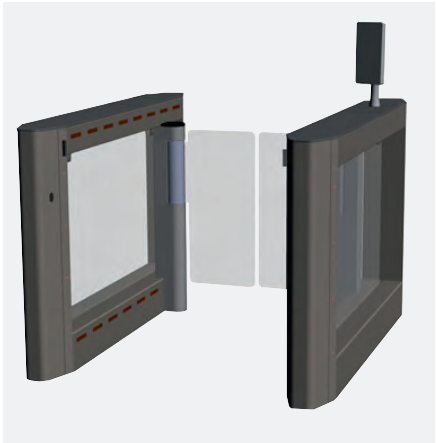


Рис. 1. Схема турникета с ИК-датчиками (барьерами) и встроенной системой видеоаналитики

Одно из основных преимуществ НС заключается в возможности параллельного функционирования её элементов,

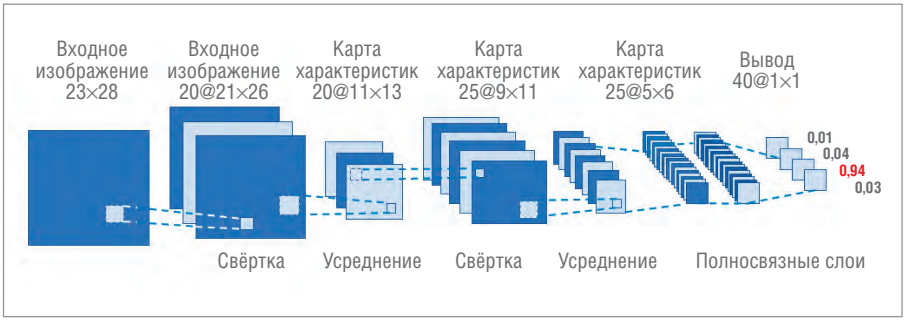


Рис. 2. Архитектура многослойной нейронной сети для распознавания изображений

что существенно повышает эффективность решения задачи. Обучение нейронных сетей упрощает выбор ключевых признаков, их весовых коэффициентов и связей между ними.

Чаще всего в таких случаях применяют многослойные нейронные сети, которые состоят из последовательно соединённых слоев, нейрон каждого из которых своими входами связан со всеми нейронами предыдущего слоя, а выходами – последующего.

Распознавание общего изображения, в частности сотрудника, проходящего авторизацию в интеллектуальном турникете с помощью биометрии, проводится с помощью многослойной нейронной сети, архитектура которой представлена на рис. 2. Нейрон с максимальной активностью (цифра 1) указывает на принадлежность к распознанному классу. Нейронная сеть с одним решающим слоем способна формировать линейные разделяющие поверхности, что значительно сужает круг решаемых задач, в частности, такая сеть не сможет решить задачу типа «исключающее или». НС с нелинейной функцией активации и двумя решающими слоями позволяет формировать любые выпуклые области в пространстве решений, а с тремя решающими слоями – области любой сложности, в том числе и невыпуклой. Обучение многослойных нейронных сетей осуществляется с помощью алгоритма обратного распространения ошибки. Такой алгоритм является разновидностью градиентного спуска в пространстве весов и обеспечивает минимизацию суммарной ошибки сети:

$$\Delta W = -\alpha \frac{dE}{dW}, \quad E = \frac{1}{2}\sum_j (y_j - t_j)^2,$$

где y_j – выходное значение j-го нейрона сети, t_j – эталонное значение выходов сети.

Скорректированные значения весов передаются от входов к выходам. Алгоритм обратного распространения является NP-трудным, поэтому время обучения сети увеличивается экспоненциально с ростом размерности данных.

Поскольку в данном случае в интеллектуальном турникете эталонные значения распознавания посетителей известны, происходит обучение сети реконструкции поданного на вход изображения, на скрытых нейронах сети формируется сжатое представление такого изображения, что может быть отнесено к классу методов самообучения.

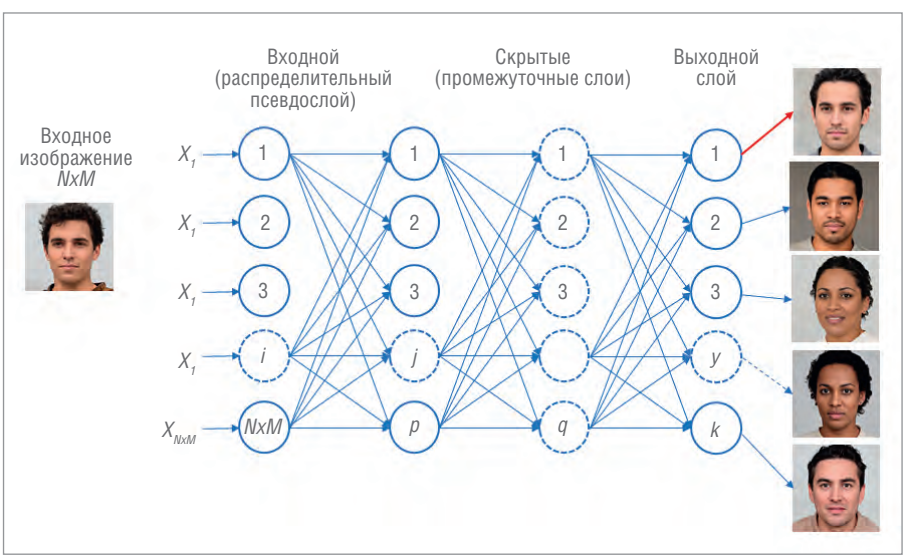


Рис. 3. Архитектура многослойной сверточной нейросети

Перед началом обучения многослойной нейросети сначала производится случайный выбор весовых коэффициентов. Поэтому допускается применение двух разных обученных нейросетей, этот метод часто применяется при распознавании лица по изображению: создаётся набор (коллектив) сетей, обученных решать одну и ту же задачу различными способами. Обобщённое, полученное таким методом, решение точнее и надёжнее, чем решение единственной нейронной сети.

В случаях, когда интеллектуальному турникету вслед за ИК-датчиками необходимо распознать сначала контур человека, чтобы убедиться, что в створе находится один посетитель, а затем провести распознавание его по лицу, чаще всего используют свёрточные нейронные сети. В классической многослойной нейронной сети межслойные нейронные соединения являются полносвязанными, изображение представлено в виде n-мерного вектора, не учитывающего ни двумерной локальной организации пикселов, ни возможностей деформации образа. Архитектура свёрточной нейросети представлена на рис. 3. В свёрточной нейросети используются локальные рецепторные поля (обеспечивают локальную двумерную связность нейронов), общие весовые коэффициенты (обеспечивают детектирование отдельных черт лица, находящихся в любом фрагменте изображения) и иерархическая организация с пространственными подвыборками (Spatial subsampling).

Свёрточная нейросеть обеспечивает частичную устойчивость к изменениям масштаба, смещениям, поворотам, смене ракурса и прочим искажениям захвата изображения камерами интеллектуального турникета.

Слои подразделяются на два типа: свёрточные (Convolutional) и подвыборочные (Subsampling), чередующиеся друг с другом. В каждом слое имеется набор из нескольких плоскостей, причём нейроны одной плоскости имеют одинаковые весовые коэффициенты, поступающие ко всем локальным участкам предыдущего слоя (как в зрительной коре человека), изображение предыдущего слоя «сканируется» небольшим окном и «взвешивается» набором весовых коэффициентов, а результат отображается на соответствующий нейрон текущего слоя. Таким образом, плоскости называются картами характеристик (feature maps), каждая из них выделяет «свои» участки изображения в

любом месте предыдущего слоя. Следующий за свёрточным подвыборочный слой уменьшает масштаб плоскостей за счёт локального усреднения значений реакции слоя на выходах нейронов, таким образом достигается иерархическая организация свёрточной нейросети. Последующие слои извлекают более общие характеристики, меньше зависящие от искажений изображения. Обучение свёрточной нейронной сети проводят стандартным методом обратного распространения ошибки. Применение многослойной и свёрточной нейросетей показало существенные преимущества распознавания как силуэтов людей, так и лиц как по скорости, так и по надёжности классификации. Полезным свойством применения нейросетей является и то, что характеристики, формируемые на выходах верхних слоев структуры, могут применяться для классификации по методу ближайшего соседа для образов, отсутствующих в обучающем наборе. Для подобных систем характерны высокая скорость обучения и быстродействие. Продолжение статьи читайте в следующем выпуске журнала. ●

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

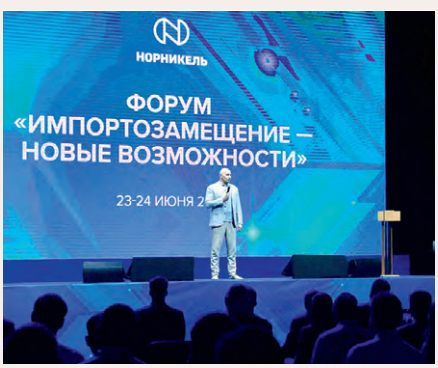
НОВОСТИ реклама НОВОСТИ реклама НОВОСТИ реклама

Компании «Адвантикс» и «Норильский никель» заключили меморандум о намерениях стратегического партнёрства

23–24 июня 2022 года в Норильске впервые состоялся форум «Импортозамещение – новые возможности», организованный компанией «Норникель». В форуме приняли участие около 200 участников из более чем 100 крупнейших технологических компаний России, Казахстана и Белоруссии, а также представители федеральных, краевых и муниципальных органов власти. В течение двух дней участники форума обсуждали способность отечественной промышленности обеспечить потребности «Норникеля» и других крупных российских предприятий всеми необходимыми материалами и оборудованием.

В текущей ситуации многие крупнейшие компании активно начинают замещать иностранное оборудование российскими аналогами. Компания «Адвантикс» на протяжении многих лет активно сотрудничает с компанией «Норникель», поставляя отечественное оборудование для самых экстремальных условий эксплуатации. Благодаря надёжной конструкции, расширенному температурному диапазону и высокой производительности изделия AdvantiX широко применяются на удалённых объектах за полярным кругом.

«Специфика работы с такими предприятиями, как “Норникель” – удалённые объекты в экстремальных погодных условиях, которые сложно регулярно обслуживать, при этом критически важна их беспрерывная работа. На форуме активно обсуждалось развитие по направлениям в сферах механических технологий, энергетики, автоматизации и цифровизации, горного производства, самоходной горной техники и транспорта. Во многих направлениях мы можем активно помочь создать импортозамещённую базу, ведь наша миссия – поставлять высокотехнологичное оборудование, которое обеспечивает беспрерывную работу в сложных условиях с минимальным обслуживанием. Мы активно продолжаем сотрудничество с “Норникелем”, развивая новые решения для их сложных задач, и рады, что данное сотрудничество будет развиваться», – комментирует Алексей Петренко, генеральный директор «Адвантикс».



Закономерным результатом форума стало заключение компаниями «Адвантикс» и «Норильский никель» меморандума о намерениях стратегического партнёрства.

Предметом меморандума является установление отношений стратегического партнёрства, развития долгосрочного эффективного сотрудничества с целью реализации концепции по импортозамещению продукции, потребляемой Заполярным филиалом компании «Норильский никель». Согласно заключённому документу, компании договорились оказывать взаимную консультативную, экспертную, организационно-методическую и информационную поддержку, предпринимать совместные действия по реализации концепции импортозамещения. ●

Кабельные вводы с IP68 от компании Degson Electronics

Известный производитель электротехнических клемм, реле и промышленных контроллеров компания Degson Electronics (КНР) постоянно расширяет номенклатуру поставляемой продукции и предлагает металлические и пластиковые кабельные сальники для организации ввода кабелей в промышленные шкафы и корпуса без потери их герметичности. Кабельные вводы выполнены из никелированной латуни или нейлона и имеют уплотнительный элемент из бутадиен-нитрильного каучука (NBR), что обеспечивает возможность их эксплуатации при температуре окружающей среды от –40 до +100°C. Кабельные вводы могут иметь наружную установочную резьбу типа PG (диаметром от PG7 до PG48) или метрическую с шагом 1,5 мм (диаметром от M12 до M63) и могут герметизировать любые кабели диаметром от 3 до 44 мм, обеспечивая степень защиты от проникновения воды и пыли до IP68. ●