Узнать по походке

Биометрия давно проникла в сюжеты книг, фильмов и в мечты граждан о будущем. Но так и не появилась в полной мере на предприятиях, за исключением, пожалуй, банковской сферы. Однако за полгода сразу две сети ритейла – «Азбука Вкуса» и «Дикси» – запустили у себя пилотные проекты, связанные с биометрическими данными. Покупатели премиальной сети получили возможность оплатить покупки, приложив палец к POS-терминалу. А в «Дикси» установили терминалы учета рабочего времени, которые сканируют папиллярный узор пальцев сотрудников. Разберемся, почему биометрия становится модной.

АВТОР: Наталья Николаева

Биометрических методов, позволяющих идентифицировать человека, множество. Часть из них ориентируется на статические параметры, такие как папиллярный узор на пальцах, сетчатка или радужка глаза, ДНК, геометрия лица, рук и даже рисунок вен или форма ушной раковины. Эти параметры неизменны, если только человек не получил какой-либо травмы или не заболел слишком серьезно. Другие методы основываются на динамических параметрах, например, анализируются голос, почерк, походка, даже запах! Создатели последнего – совсем молодого – метода утверждают, что прибор, определяющий индивидуальный рисунок запаха тела, не собьешь ни дезодорантами, ни мылом.

Методы различаются между собой сложностью, стоимостью необходимого оборудования, а также частотой допускаемых ошибок и устойчивостью к обману. «Статическая биометрия распознает человека по частям тела: отпечаткам пальцев, лицу или глазам. Обвести вокруг пальца такую систему достаточно легко, – утверждает Шандор Балинт, руководитель отдела защиты прикладных задач компании Balabit. – Поведенческая биометрия базируется на знании, что вы делаете или как вы это делаете: на динамике нажатия на клавиатуру или кнопку мышки. Сымитировать такое намного сложнее».

Разумеется, далеко не все перечисленные методы биометрии подходят для ритейла, и дело тут не только в стоимости того или иного метода. «Очевидно, что возможно применять не все виды биометрической идентификации из доступного многообразия, которое к тому же постоянно расширяется, – делится подробностями Владимир Иванов, директор по развитию компании «Актив». – Например, идентифицировать покупателя по ДНК, извлеченной из пробы крови, в магазине никто не будет. Будут использоваться доступные методы: отпечатки пальцев, форма головы, ушной раковины, рисунок вен ладони. Эти методы отличаются тем, что идентификацию можно проводить достаточно быстро в публичном месте, не доставляя дискомфорта клиенту».

Наиболее заинтересованные в использовании любого из приведенных методов – это специальные и криминологические службы, которым необходимо быстро и безошибочно выделять нужного человека из толпы, а также компании, где есть секретные разработки, доступ к которым могут получить лишь авторизованные сотрудники. Зачем вообще нужна какая-либо биометрическая система ритейлу?

Подобно тому, как много методов используется в биометрии, существует и множество применений подобных систем. Первое из них – обеспечение безопасности, которая играет важную роль и в торговой сфере. «Биометрические технологии используются в различных сферах бизнеса, в первую очередь в целях повышения безопасности: для распознавания лиц, контроля доступа. Ритейл здесь не исключение, – соглашается Виталий Кузнецов, управляющий партнер компании Office Anatomy. – Видеоаналитика позволяет собирать статистику посещения каждой точки, идентифицировать VIP-клиентов или, наоборот, нежелательных посетителей, получать визуализацию маршрутов передвижения людей. В том числе можно оценивать правильность расположения товарных групп на полках, делать выводы об эффективности планирования торговых площадей. Кроме того, системы видеоаналитики позволяют существенно сокращать кражи, которые являются одной из основных серьезных проблем розничной торговли. К слову, общая доля потерь оценивается в 50 млрд руб. в России ежегодно».

ДВА ПУТИ

«Биометрия, а вернее, биометрическая идентификация, стала в последнее время модной темой. Ею увлечены банки, платежные системы, розничная торговля и сфера услуг – все бизнесы, работающие с частными клиентами. Всю их совокупность мы и будем называть розницей для краткости, – предлагает Владимир Иванов. – Можно указать на два совершенно разных пути применения биометрической идентификации в рознице. Линия раздела проходит в точности по прилавку, по границе, разделяющей персонал и клиентов».

По словам Владимира Иванова, для персонала обычно внедряют различные системы контроля присутствия на рабочем месте и учета рабочего времени. Такие системы достаточно распространены и уже имеют солидную историю применения. С клиентами же все гораздо интереснее. Бизнес заинтересован в том, чтобы повышать уровень обслуживания клиентов, формировать для них индивидуальные предложения и в итоге зарабатывать больше денег. Например, розничный магазин стремится сделать процесс оплаты товаров более удобным и заменяет банковскую карту отпечатком пальца.

Именно такой проект мы видим в «Азбуке Вкуса». Покупатель получил возможность оплатить покупки, приложив палец к специальному POS-терминалу. Там отпечаток сканируется биометрическим сканером. Чтобы верификация оказалась возможной, клиент должен предварительно зарегистрироваться на кассе и привязать отпечатки нескольких своих пальцев к своей же банковской карте (Visa

или Master Card). «Для покупателей это прежде всего удобство, потому что не надо носить с собой ни деньги, ни банковскую карту, ни телефон, – рассказывает Георгий Михайлов, директор по инновациям компании «Азбука Вкуса». – Для нас это еще одна возможность добиться идеального shopping experience». По его словам, клиенты магазина реагируют очень живо и с интересом. «С точки зрения безопасности можно сказать, что биометрия – более надежная технология, чем, например, ввод пин-кода для банковской карты, – добавляет Георгий Михайлов. – Данные о пин-коде можно украсть, а вот отпечаток ваших пальцев индивидуален. Партнером здесь выступает «Сбербанк», поэтому никаких нареканий к системе нет. Сейчас проект реализован в магазине на Нахимовском проспекте, 61, который имеет сформировавшуюся аудиторию. Поэтому основными пользователями новой технологии стали постоянные клиенты этого супермаркета. Дальнейшие планы по развитию этой технологии будем обсуждать уже после Нового года, когда мы подведем итоги пилота».

Какие плюсы получит ритейл от внедрения? «Главное преимущество – удобство. Намного проще, а иногда даже быстрее приложить палец к сканеру, чем тянуться за кошельком, искать наличные или карту, вводить пин-код, – объясняет Шандор Балинт. – Еще один очевидный плюс – меньше упущенных возможностей для бизнеса. Даже если человек забыл дома кошелек, отпечаток пальца у него всегда с собой, а значит, он в любом случае сможет совершить покупку. Некоторых может привлечь новизна биометрических технологий, и это тоже может повлиять на продажи».

Сеть «Дикси» подошла к биометрии с другой стороны. Здесь объектом стали не покупатели, а сотрудники торговых точек. Однако методика та же – сканирование папиллярного узора. Терминалы учета времени отмечают приходы и уходы сотрудников, а те регистрируют свое появление с помощью отпечатка пальца. «Проект продемонстрировал повышение трудовой дисциплины в пилотируемых магазинах, а также позволил автоматизировать процесс учета рабочего времени для департамента по работе с персоналом, – отмечает Екатерина Куманина, директор по корпоративным и внешним связям ГК «Дикси». – Биометрическая система практически исключает лазейки для злоупотреблений. До внедрения этого проекта мы пробовали различные инструменты, но все они не демонстрировали требуемой эффективности. Например, электронные карты доступа сотрудники могут просто передавать друг другу. Количество ошибок сегодня не превышает 2%. Для разрешения спорных случаев компания использует дополнительные инструменты – видеофиксацию или журнал».

В «Дикси» уже перешли от пилота к реализации полномасштабного проекта. Системой оснащено 2600 магазинов сети. Что касается окупаемости, то, как комментирует Екатерина Куманина, эффект от внедрения биометрии сложно оценить. «Система является стратегическим проектом, так как автоматизированный учет и дальнейшее сопоставление данных биометрии с показателями продаж предоставляет дополнительные возможности для эффективного управления персоналом. Соотнося продажи с количеством персонала в магазине и временем их работы, мы можем определять эффективность работы, выявлять, где людей достаточно, где мало, эффективно рассчитывать KPI», – поясняет она.

ГОНКА ЛИДЕРОВ

Два описанных выше проекта работают, используя отпечатки пальцев. Неудивительно, ведь это одна из старейших методик. Снимать такие отпечатки для последующей идентификации их хозяина начали еще в XIX веке, пусть и без применения информационных технологий. Сейчас метод распознавания по папиллярному узору – самый распространенный. И если начиналось все с криминалистики, то заканчивается дело бизнесом. Технологию начали использовать в смартфонах и планшетах. «Использование биометрических данных – это новый тренд в общении человека и компьютера, который сейчас активно распространяется в мире, – объясняет Тамара Морозова, генеральный директор компании «РекФэйсис». – Мы уже привыкли к тому, что подтверждаем операции в онлайн-банкинге с помощью отпечатка пальца, разблокируем телефон с помощью отпечатка пальца, в новых моделях телефонов Samsung это будет делаться уже с помощью сканера радужки глаза, в новых версиях операционной системы iOS есть сервис по поиску и структурированию фотографий по конкретному человеку, Instagram внедрил поиск людей по фотографиям».

Как только технология проникает на пользовательский уровень, она становится более привлекательной и для бизнеса, ведь теперь это что-то знакомое и любопытное. То, что может быть использовано. Об этом свидетельствуют и слова Георгия Михайлова из «Азбуки Вкуса»: «В ближайшие годы биометрические платежи станут третьим вариантом оплаты наряду с наличными и банковскими картами. А что именно будет ключевым идентификатором – рассудит время. Поэтому инвестиции в развитие подобных

систем уже нельзя назвать венчурным проектом. Это требование времени. И лучше быть в роли лидеров, а не догоняющих».

«Все эти и не только эти технологии, конечно же, будут повсеместно внедряться в ритейле, как в отрасли, которая более всех остальных работает с огромным количеством людей, – подтверждает Тамара Морозова. – С помощью биометрии ритейл сможет узнавать своего клиента «в лицо» еще при входе в магазин и вести с ним более адресный диалог, сможет упростить для людей программы лояльности, обеспечить бескарточную систему платежей; продолжать можно очень долго. Конечно, ритейл как никакой другой рынок видит перспективы применения биометрии в ритейле, и интерес со стороны как крупных, так и мелких ритейлеров постоянно усиливается».

ГАДАНИЕ ПО ЛИЦУ

Сервис хочет знать клиентов в лицо в буквальном смысле этого слова. «Распознавание лиц является одним из наиболее комфортных способов идентификации человека на основе его физиологических характеристик, – говорит Виталий Кузнецов. – Получение данных не затруднено, и от человека не требуется производить какие-либо дополнительные действия (в отличие, например, от дактилоскопии). В плане взаимодействия с клиентами бесконтактный метод биометрических решений (распознавание по геометрии лица) видится более приоритетным».

По словам Тамары Морозовой, количество возможных сценариев применения распознавания лиц в продуктовом ритейле достаточно большое, и рассказывать о них можно долго. «Я приведу несколько наиболее популярных сценариев. Первый из них – это привязывание изображения человека к программе лояльности, когда человек подходит на кассу, система сама его распознает и в зависимости от уровня карты лояльности делает ему скидку/присваивает баллы. В магазинах, ориентированных на работу менеджеров с клиентами, это может быть процесс «узнай своего клиента в лицо» и в соответствии с имеющейся в сети программой рекомендованных покупок более адресная работа с ним», – делится она.

В первую очередь такие решения используются для обеспечения безопасности. «Один из наших продуктов от Herta Security – BioSurveillance – предназначен для обеспечения безопасности в многолюдных местах, например, в торговых центрах, – рассказывает Виталий Кузнецов. –

Решение позволяет обнаруживать несколько лиц одновременно в режиме реального времени, анализирует несколько камер в одно и то же время, а также включает в себя моментальную обработку изображений, полученных при помощи видеозахвата. Если говорить о России, BioSurveillance внедряется в строящемся логистическом комплексе «Радумля», в одном из крупнейших оптово-распределительных центров площадью около 750 000 кв. м».

Однако распознавать лица можно не только ради обеспечения безопасности магазина, но и для повышения привлекательности торговой точки в глазах своих покупателей. В этом случае биометрия помогает распознать не само лицо как таковое, а, например, эмоции, которые испытывает тот или иной покупатель. «Лояльность клиента включает в себя несколько составляющих: эмоциональную лояльность, когда людям нравится этот бренд, этот магазин, и экономическую лояльность, когда клиенту выгодно пользоваться услугами именно этой компании, – разъясняет Сергей Юдицкий, генеральный директор компании ProLAN. – Но есть и третий фактор, когда посещение точки продаж оставляет положительный эмоциональный след. Корреляция между повторными продажами и тем, что клиент удовлетворен, не больше 40%. Продажи от того, что клиенту выгодно тут покупать, тоже не слишком растут. Не хватает вот этого третьего элемента – наличия эмоционального следа у покупателей. Наш «Монитор эмоций» основан на использовании метода объективного маркетинга. Мы снимаем карту того, что реально происходит».

Как пояснил Сергей Юдицкий, идея заключается в следующем. Существуют два психологических эффекта, которые важны для ритейла. Первый – «эмоциональное заражение». Если я доволен качеством обслуживания, и тут продавец мне улыбнулся – я инстинктивно улыбнусь в ответ. Если я недоволен, я в ответ улыбаться не буду, улыбка продавца оставит меня равнодушным. Второй эффект называется наведенным (Affect Infusion). «Под воздействием разных эмоций мы по-разному оцениваем качество обслуживания. Поэтому чем лучший эмоциональный след у нас остается от магазина, тем больше вероятность того, что мы придем сюда снова. Улыбка, вызываемая положительными эмоциями, помогает вырабатывать эндорфины, и организм запоминает – там было хорошо», – утверждает Сергей Юдицкий. Но если ритейлер хочет управлять эмоциональным состоянием клиента, то нужно для начала это состояние измерить.

«Есть точка контакт между продавцом и покупателем, – описывает Сергей Юдицкий. – Там стоит камера, которая направлена в сторону покупателя. В корпоративном стандарте продавца записано, что в конце покупки сотрудник должен послать некий положительный импульс покупателю, например, сказать что-то хорошее и улыбнуться. Если мы делаем это неформально и если покупатель удовлетворен обслуживанием, он автоматически улыбнется в ответ. Это настроение покупателя фиксируется нашим решением, сохраняется «эмоциональный снимок». Там записан начальный эмоциональный фон покупателя и его эмоции в течение 30 секунд. Таким образом, у нас есть объективные данные по покупателю, который прошел через точку контакта. Лучше всего этот метод применять в бутиках, где продавцы хорошо замотивированы, а покупательский поток не слишком велик. Такой «сервис с улыбкой» (Service with a smile) помогает повысить продажи на 30%. И нужно понимать, что эти проценты возникают не за счет того, что люди начинают покупать больше, когда продавец им улыбается. Это иллюзия. Больше продается потому, что клиент возвращается снова и снова. При этом мы можем измерять как общий эмоциональный фон, так и всплеск эмоций, их изменение. Эта информация может использоваться и для управления клиентоориентированностью продавцов, и для управления лояльностью покупателей (как объективная интегральная оценка клиентского опыта)».

Еще одна сфера применения распознавания лиц в ритейле – это определение маркетинговой стратегии с помощью измерения состава посетителей. «Сейчас чаще всего используют технологии, которые считают посетителей, не предоставляя качественный портрет аудитории, – говорит Виталий Кузнецов. – Но видеоаналитика позволяет не только собирать статистику посещения каждой точки. Система BioMarketing, предназначенная для маркетинговых целей, определяет возраст, пол, этническую или расовую принадлежность, наличие очков и др. На основании этих данных можно рекламировать продукты под определенную категорию людей. Например, для возрастной группы до 25 лет запускается один рекламный видеоролик, а для людей возрастом до 50 – другой».

ЛОЖКА ДЕГТЯ

Описание любой технологии всегда очень интересно выглядит на бумаге и красиво – в промороликах. Однако в жизни пользователи неизменно сталкиваются с кучей сложностей. Например, в Интернете несложно найти множество отзывов о том, как компания не справилась с биометрическими технологиями у себя в офисе. Скажем, если речь шла о регистрации приходов и уходов, описываются ситуации, когда за пять минут до начала рабочего времени у сканеров образуется толпа сотрудников, которые стремятся не опоздать. Тот сотрудник, кто будет возиться со своим пальцем чуть дольше обычного, услышит о себе нелицеприятные отзывы, а уж если система дает сбой и не принимает первую и вторую попытки «зачекиниться» на рабочем месте с помощью отпечатка пальцев, толпа просто звереет – ведь всем, кто зарегистрировался не вовремя, грозит штраф. Еще одна проблема – настройки сканера. Люди жалуются, что при высоких параметрах защиты система «не узнает» сотрудника, особенно если у него есть порезы на пальцах, следы от клея и так далее, а если эти параметры понизить, то система просто путает сотрудников.

Что касается ошибок, есть сферы деятельности, чрезвычайно критичные к таким ошибкам, и бизнес, который не теряет прибыли из-за небольших погрешностей в идентификации. Об этом говорит Тамара Морозова: «Например, если мы говорим об инструменте для up-sale, то там наличие даже одной ошибки на 100 000 посетителей некритично и не нанесет никакого урона ритейлеру, поэтому можно использовать один алгоритм распознавания лиц. А если мы говорим, например, о подтверждении тех или иных финансовых опера-

ций, где возможны попытки сознательной компрометации со стороны людей и где цена ошибки более высока, можно использовать идентификацию по 3D-модели лица. Использование мультибиометрической платформы позволяет предлагать заказчику гибкий инструмент под его потребности. В зависимости от сферы применения и критичности ошибок можно использовать несколько алгоритмов или использовать наиболее надежные биометрические технологии, чтобы свести процент ошибок к нулю».

В любом случае каждый производитель стремится свести ошибки своих систем к минимуму. А вот на чем стоит остановиться и рассмотреть вопрос подробнее, так это на возможности подделки биометрических данных. «Очень важно помнить, что биометрия – это широкая область научной дисциплины, а не только технология, – поясняет Шандор Балинт. – И одно из основных направлений исследований – изучение физиологических особенностей человека, которые можно использовать для его идентификации. Большую часть систем, использующих для идентификации отпечатки пальцев, ладоней, схему кровеносных сосудов, снимок радужки глаза, распознавание лица, голоса, особенности походки, динамику набора текста на клавиатуре, можно обмануть тем или иным способом, причем иногда это до смешного элементарно. Например, некоторые сканеры отпечатков можно легко обмануть с помощью тонкой резиновой пленки, надетой на палец, а программы распознавания лиц иногда не отличают реального человека от фотографии. Поэтому лучше рассматривать биометрию как дополнительную броню, а не как способ стопроцентно надежной и безопасной аутентификации».

«Представьте такую ситуацию: мужчина с распечатанной фотографией лица другого человека, приложив ее к своему лицу, проходит через турникет. В этом случае система идентифицирует лицо с фотографии, если этот снимок очень хорошего качества. Но мы также понимаем, что в реальной жизни вряд ли кто-то воспользуется этим способом. Ведь незамеченным этот трюк не останется, – парирует Виталий Кузнецов. – Конечно, существуют риски неточного распознавания, если, к примеру, у человека закрыто больше половины лица шарфом. А вот наличие усов, очков, бороды не является помехой для распознавания. Следует понимать, что есть и плюсы, и минусы в любой системе. В случаях, когда риски велики, всегда можно применить двухфакторную аутентификацию (например, распознавание по отпечатку пальца или по радужной оболочке глаза)».

С коллегами согласен и Владимир Иванов. На биометрию пока нельзя положиться в полной мере. «Существует ряд опасностей, связанных с подменой понятий, – говорит он. – Дело в том, что маркетологи от биометрии пытаются представить биометрические способы идентификации как совершенно безопасные. Нюанс состоит в том, что биометрические данные представляют собой идентификатор субъекта, то есть человека. Грубо говоря, это некоторый набор цифр, зависящий от биометрических параметров, связанный с учетной записью в информационной системе. Набор этот со всей очевидностью постоянен, поскольку изменить отпечатки пальцев, к примеру, человек при всем желании не может. Авторизацией операций в информационной системе занимается программный код, для которого человек существует исключительно в виде идентификатора, то есть набора цифр. По этому идентификатору программа не может отличить легального пользователя от нелегального, если датчик биометрической информации сообщает о том, что проверяемые параметры с нужной вероятностью соответствуют эталонным значениям, которые хранятся в системе. Датчик биометрической информации не может с абсолютной точностью считать данные, чтобы они соответствовали эталону, поэтому процесс биометрической идентификации всегда носит вероятностный характер. Этим могут пользоваться злоумышленники, изготавливая имитаторы: муляжи пальцев с отпечатками, синтезированный голос и т.п. Если имитация получается достаточно точной, можно считать, что биометрические данные человека для данной системы скомпрометированы и ими нельзя пользоваться. При изготовлении имитатора важно лишь то, чтобы с нужной степенью точности воспроизводились только контролируемые параметры оригинала, то есть не нужно изготавливать имитатор, абсолютно идентичный оригиналу. Ограничивающим фактором, по сути, является только стоимость изготовления имитатора той или иной характеристики».

По словам Владимира Иванова, наблюдается прямая зависимость между стоимостью датчиков, считывающих биометрические параметры, количеством параметров и точностью распознавания. В пределе получается ситуация, когда стоимость оборудования для снятия биометрических параметров, учитывающего при распознавании множество второстепенных факторов, может стать слишком большой. «Фактически же мы имеем ситуацию, когда в рамках ограниченного бюджета закупается дешевое оборудование, уязвимое к малобюджетным атакам, – сетует он. – При реализации проектов нужно обязательно анализировать риски и не применять уязвимые системы в случаях, когда потери могут быть неоправданно большими».

Каков же выход? Очевидно, что должно быть нечто, что связывало бы биометрические данные человека с его личностью. Как говорит Владимир Иванов, самый распространенный способ – это фактор знания, то есть секрет, известный человеку. Для банковских карт, например, таким секретом является PIN-код. То есть сочетание биометрических данных со знанием пароля будет более безопасным. Другим выходом может быть применение комплексных способов идентификации, для которых трудно изготовить имитатор. Например, сочетание распознавания походки, фигуры и лица человека может быть достаточно надежным способом.

«Также существует и правовая проблема использования биометрии, – добавляет Владимир Иванов. – Биометрические данные могут являться персональными данными. Работа с ними регулируется 152 ФЗ и подзаконными актами. Это всегда нужно учитывать при реализации проектов. Как бы то ни было, не следует забывать о том, что биометрические данные – это не пароль и не криптографический ключ, и сменить их в случае компрометации не получится. Это может доставить клиенту массу неудобств в дальнейшем».

Действительно, когда скомпрометирован пароль, система немедленно предлагает пользователю изменить его на новый. С биометрическими данными так не получится. «В отличие от пароля, который можно изменить в любой момент, биометрические показатели у человека одни и те же, – развивает мысль Шандор Балинт. – Если компания решит их использовать, вы не сможете изменить свои параметры, с помощью которых будете проходить проверку подлинности. Хотя вы, конечно, можете выбрать, каким пальцем, к примеру, разблокировать айфон, а каким – получить доступ в офис».

По мнению Шандора Балинта, если один и тот же биометрический показатель используется для проверки разными компаниями, например, ваш работодатель и банк идентифицируют вас по отпечатку, это может стать поводом для спекуляции вашими данными мошенниками. «И хотя это пока что не самая распространенная проблема, в будущем с распространением этой технологии нам будет чего опасаться», – заключает он. ◆