

БИОМЕТРИЧЕСКИЕ ИНСТРУМЕНТЫ ДЛЯ БИЗНЕСА

© Рудская Е.Н.^{*}, Кобылат А.О.[♦]

Донской государственный технический университет, г.Ростов-на-Дону

В статье рассматриваются вопросы эволюции биометрических технологий, их виды и проблемы коммерциализации. Исследованы основные виды биоидентификации, выявлены особенности их применения в финансовой сфере. Также обоснованы рекомендации по выработке внутренней политики компаний, применяющих биометрию. Соавтор Кобылат А. занимается разработкой прототипов устройства для измерения биометрической информации.

Ключевые слова: биометрия, биоидентификация, аутентификация, биометрия в бизнесе.

Биометрические технологии уже давно превратились из простых средств идентификации в инструменты для бизнеса.

Задача биометрических технологий – дать четкий ответ на вопрос: кто? Вопрос кто был актуален во все времена – и первые попытки решить его за счет присущих каждому человеку особенностей относят еще к каменному веку, когда авторы наскальной живописи «подписывали» свои произведения отпечатками ладоней.

Наиболее интересные моменты развития биометрии представлены в табл. 1 [4, с. 34-36].

Таблица 1

Развитие биометрии

Дата	Изобретение
1877	Британский полицейский чиновник Уильям Гершель во время службы в Индии, имея трудности с запоминанием лиц, использует папиллярный узор для идентификации своих подчиненных из числа местного населения и тем самым закладывает основы дактилоскопии.
1892	Френсис Гальтон, племянник Чарльза Дарвина, публикует классический труд «Отпечатки пальцев», где констатирует неизменность папиллярного узора в течении жизни человека и доказывает, что вероятность совпадения узора у двух разных людей стремится к нулю. Через три года по его состоянию Скотланд-Ярд приступает к дактилоскопированию преступников и подозреваемых. Начинается бурное развитие дактилоскопии.
1902	Впервые в мире отпечатки пальцев используются в английском суде как доказательство вины преступника.
1936	Американский офтальмолог Фрэнк Барч предлагает использовать узор на радужке глаза, как уникальный идентификатор для определения личности человека. Лишь пятьдесят лет спустя идею доводят до патента и лабораторных исследований.
1965	Американец Вудро Бледсо, один из пионеров искусственного интеллекта, работая по правительственному заказу, строит первую автоматизированную систему распознавания лиц.

^{*} Доцент кафедры «Экономика», кандидат экономических наук, доцент.

[♦] Студент факультета Приборостроения и технического регулирования.

Продолжение табл. 1

Дата	Изобретение
1980	На массовом рынке появляются впервые практически пригодные биометрические системы. В качестве биоидентификатора используется геометрия кисти.
1992	По инициативе и под контролем Агентства национальной безопасности США создается Biometric Consortium-для координации биометрических исследований и их коммерческого применения между правительством, промышленностью и научным сообществом. Первые десять лет консорциум работает буквально в режиме военной секретности.
1996	На Олимпийских играх в Атланте участников сортируют с помощью биометрической системы геометрии рук.
1998	ФБР запускает биометрическую базу данных CODIS, хранящую информацию обо всех ДНК-отпечатках, найденных в ходе следственных мероприятий.
2002	Международная организация по стандартизации (ISO) формирует рабочую группу для поддержки выработки общих стандартов биометрических технологий.
2005	Samoff Corp. демонстрирует систему фотографирования радужки глаза, способную работать незаметно для человека.
2013	Индия становится обладателем крупнейшей мультимодальной (то есть использующей сразу несколько индикаторов) биометрической базы данных Aadhaar. В перспективе в ней должны оказаться записи, идентифицирующие большую часть населения страны.

Все биометрические технологии выросли на единственном предположении: каждое живое существо наделено некоторыми уникальными особенностями, присущими только ему. Эту особенность называют биометрическим идентификатором.

Науке известны два типа таковых: физиологические, то есть относящиеся к форме тела и его устройству (отпечатки пальцев, радужная оболочка, геометрия лица) и поведенческие (манера печати на компьютерной клавиатуре, особенности вождения автомобиля).

На рис. 1 [4, с. 38] представлена структура мирового рынка биометрических технологий с точки зрения оборота. Самый большой процент занимают дактилоскопические системы (идентификация изображения).

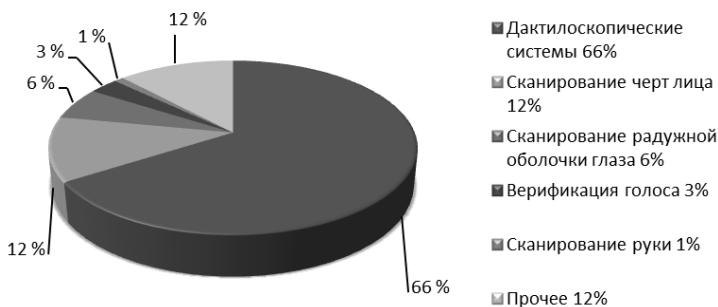


Рис. 1. Структура мирового рынка биометрических технологий

Поведенческая биометрия еще не вышла из стен лабораторий и пока сильно уступает в скорости и качестве физиологической. Но именно здесь,

возможно, нас ожидают наиболее перспективные технологические прорывы в будущем.

На диаграмме рис. 2 [4, с. 33] представлен рост мирового рынка биометрических технологий. С 2009 года потребление биометрических продуктов выросло примерно на 6 млрд.долл, или в два раза.

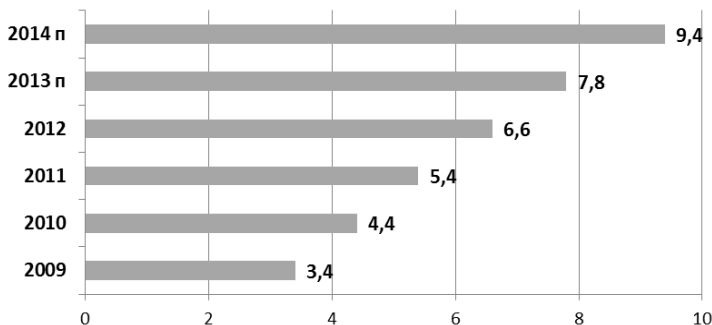


Рис. 2. Рост мирового рынка биометрических технологий, млрд. долл.

Существует несколько видов идентификации личности, такие как:

1. распознавание по глазу;
2. технология трехмерного сканирования лица;
3. распознавание голоса;
4. поведенческая биометрия.

Первый вид идентификации – распознавание по глазу. Наталья Ульянова подробно рассматривает этот вид в статье «Открой личико!» [7, с. 48-50]. Такая идентификация достаточно надежна – но и она не дает стопроцентных гарантий. В 2012 на конференции по безопасности Black Hat была обнародована научная работа, посвященная воссозданию чужой радужки в виде картинки или контактной линзы. Наиболее успешным воплощением данной технологии является IrisAccess, которую можно приобрести за 400 000 рублей.

Следующий тренд – технология трехмерного сканирования лица. Биометрическая разработка компании Artec Group (США) «узнает» людей прямо на ходу с помощью технологии трехмерного сканирования лица. Причем новая прическа, солнечные очки, отросшая борода и усы ей не помеха [1, с. 44].

Ее физическое воплощение – металлическая стела высотой чуть больше метра. В стелу вмонтирована 3D камера, которая начинает снимать приближающегося человека за 2 метра. Компьютер обрабатывает трехмерные снимки, сверяет их с изображениями из базы данных, а заодно дополняет базу новыми изображениями человека, с каждым разом увеличивая степень достоверности распознавания.

Эта система сейчас работает в Эрмитаже, Кремле, в аэропортах Норильска и Сочи, на предприятиях Росатома, в Сбербанке и других компаниях, её стоимость составляет 554 700 руб.

Третьим видом является распознавание голоса. Речь, голос человека – вполне надежные параметры, чтобы идентифицировать личность даже через много лет. Российская компания «Центр речевых технологий» из Санкт-Петербурга занимается такими разработками уже более 20 лет, в том числе для Мексики и Эквадора.

Биометрия по голосу хороша тем, что не зависит от языка человека, чью личность нужно установить или доказать. Здесь используется так называемая бимодальная биометрия, когда для повышения точности идентификации используется сразу 2 параметра – голос и изображение человека. Голосовые системы имеют лучшие перспективы, хотя бы, потому что для их применения массовому потребителю понадобится то, что у него и так есть – микрофон и компьютер [8, с. 40].

Однако, самой перспективной считается поведенческая биометрия. Теоретически она способна не только значительно повысить надежность идентификации, но и избавить от лишних технических сложностей. В настоящее время данная технология используется лишь как дополнение к физиологическим биометрическим технологиям.

С базовой задачей почти безошибочно идентифицировать личность биометрия справилась давно, еще в доцифровую эпоху. Теперь на повестке дня задача куда сложнее – научиться распознавать нюансы психофизиологического состояния человека. На рынок начинают выходить биометрические системы третьего поколения. Свою разработку VibraImage Виктор Минкин из петербургской компании «Элсис» относит как раз к таковым. Его система за считанные секунды вычисляет в толпе потенциально опасных людей [1, с. 46].

Еще одно применение технологии VibraImage – детекция лжи. Причем в этом случае система имеет определенные преимущества перед обычными полиграфами, поскольку работает бесконтактно. Устройство VibraImage можно приобрести за 250000 руб.

Существуют три модели использования биометрии (рис. 3) [6, с. 6]:

1. Государственные программы.
2. Программы организаций.
3. Отраслевые программы.

Крупные заказы, связанные с необходимостью реализации масштабных проектов государственного и муниципального уровня (удостоверения личности, проездные документы), не только вызвали снижение цен на такого рода технологические решения, но и стали инструментом популяризации биометрии, прежде использовавшейся лишь в узких сферах и нишах.

Показательный пример – переход целого ряда федеральных служб США, таких как Министерство внутренней безопасности, к сканированию отпечатков всех пальцев иностранных граждан, прибывающих на территорию страны. По сравнению с использовавшимся прежде сканированием отпечат-

ка одного пальца, такая процедура позволяет получить более точную информацию и ускоряет регистрацию данных. Еще недавно такие технологии считались слишком дорогостоящими, чтобы обеспечить их широкое применение. Ныне это уже тиражируемые решения.



Рис. 3. Три модели использования биометрии

Организации, начавшие использовать биометрические системы безопасности, также сумели сделать весьма любопытные выводы, основываясь на собственном опыте. Современные биометрические сенсоры весьма точны. Отчасти благодаря тому, что испытания первых решений такого рода показали: чрезвычайно важно разработать действительно надежные и эффективные процедуры проверки граждан или клиентов. Иначе смысл прохождения биометрических тестов утратится.

Некоторые общественные организации, выступающие за защиту конфиденциальности личной информации, не раз выражали обеспокоенность тем, что биометрические системы контроля могут не срабатывать, затрудняя доступ к тем или иным услугам для добропорядочных клиентов, обладающих подлинными биометрическими удостоверениями личности. Однако эти

опасения до сих пор не были подтверждены достаточно серьезными ограничениями. Хотя очевидно, что всем организациям, применяющим биометрию, все-таки необходимо иметь в запасе альтернативные способы установления личности на случай невозможности распознавания или регистрации биометрических данных (в том числе в случае сбоев аппаратного или программного обеспечения).

Нарастает и «эффект масштаба», благодаря повсеместному применению биометрических технологий, что уже оценили многие компании.

За рубежом биометрические технологии хорошо известны среди населения [6, с. 3]. Основываясь на данных опроса, проведенного компанией Unisys, являющейся одним из ведущих поставщиков биометрических решений, можно сделать вывод, что в Великобритании сегодня 56 % потребителей уже не возражают против предоставления биометрических данных в целях установления личности при совершении розничных покупок и финансовых транзакций. 95 % британцев готовы к этому (а также к сканированию отпечатков пальцев) при работе с банками и государственными службами. Общество становится все более зрелым. И это шанс для всего рынка биометрических систем.

Количество граждан в развитых странах, готовых применять биометрию, колеблется от 50 % в Германии до 66 % в Австралии. Сканирование отпечатков пальцев стало сегодня наиболее широко распространенным биометрическим методом, оставляя позади не только сканирование лиц и анализ голоса, но и использование PIN-кодов.

Дополнительное внимание к этим технологиям обеспечило введение биометрических паспортов и удостоверений личности. Сегодня биометрические технологии быстро эволюционируют благодаря финансированию со стороны служб охраны общественного порядка и обеспечения общественной безопасности. За последние пять лет, 2008-2013 гг., удалось значительно увеличить скорость считывания данных, сократить долю несправедливых отказов в доступе и ложного приема предоставленных данных. Не случайно биометрия уже практически не ассоциируется исключительно с криминалистикой, как это было еще совсем недавно.

Особый интерес к биометрии проявляет финансовая сфера. В финансовом секторе все более актуальной задачей становится и нарастающая борьба с отмыванием денег, что требует внедрения эффективных систем верификации личности каждого клиента. Биометрия могла бы сыграть важную роль в создании таких средств, особенно если бы правительства обеспечили банкам и другим финансовым организациям доступ к общенациональным базам биометрических удостоверений личности (например, в рамках федеральных программ биометрической идентификации).

Предотвращение незаконного присвоения персональных данных могло бы стать серьезным двигателем внедрения биометрических технологий,

поскольку именно этот риск напрямую влияет на результаты деятельности компаний, непосредственно взаимодействующих с потребителями не только в финансовом секторе, но и, например, в сфере розничной торговли.

По приблизительным подсчетам, масштаб убытков, связанных с незаконным использованием персональных данных в США, колеблется от 5 до 50 млрд. долл. в год [6, с. 4].

По расчетам британского правительства, вызванные мошенничеством в сфере персональных данных убытки для страны ежегодно превышают 1,7 млрд. фунтов.

Для того чтобы реализовать максимально надежные процедуры установления личности, финансовые компании всерьез анализируют перспективы замены (или дополнения имеющихся) документов, содержащих только биографические данные (таких как паспорта и свидетельства о рождении), биометрическими. Эти меры помогут повысить уровень безопасности, не требуя при этом создания новой инфраструктуры идентификации личности.

Например, клиент, личность которого уже была установлена с помощью биометрической технологии прежде, сможет представлять меньшее количество документов при открытии счета – или же открыть счет быстрее, поскольку банку потребуется меньше проверок.

На первом этапе банки и финансовые организации могли бы ввести в строй биометрические системы исключительно для операций с повышенным риском, а попутно – предложить эту технологию своим клиентам, управляющим крупными счетами, в качестве дополнительной меры безопасности. Так уже поступили некоторые банки, применив программу проверки доступа к счетам CAP (Chip Authentication Program).

Использование биометрии в качестве дополнительного метода установления личности – например, при проведении крупных финансовых операций – позволит сократить убытки.

Биометрия смогла бы заменить пароли или электронные ключи для доступа не только к компьютерным программам (таким как «клиент – банк»), но и к защищенным объектам (включая центры обработки данных или электронные биржевые системы).

Возвращаясь к самому важному вопросу о защите персональных данных, отметим, что опасения о сохранности информации поставили под вопрос эффективность технологии.

Ряд проблем, возникавших на первоначальных этапах внедрения обсуждаемых технологий, удалось преодолеть. В частности, некоторые решения распознают держателя документа по фото, что устраняет необходимость (например, в случае с такими системами, как IRIS) личного присутствия при регистрации данных.

Благодаря совершенствованию и повышению точности сканеров удалось уменьшить число ложных отказов систем, а применение более стойких алго-

ритмов шифрования и понимание того факта, что при правильном применении системы нет необходимости в постоянном хранении и передаче данных, позволили исключить целый пласт рисков, связанных с мошенничеством.

Однако каждая организация, планирующая применение биометрических технологий, – и государственная, и коммерческая, должна, прежде всего, сформулировать ключевые параметры, соответствующие ее потребностям. Тем более что выбор сегодня достаточно широк. Система проверки отпечатков всех десяти пальцев дает исключительную точность, однако, скорее всего, будет восприниматься как некомфортная покупателями розничных сетей. В свою очередь, распознавание лиц с помощью камер видеонаблюдения практически «незаметно», но коэффициент ложных отказов при использовании подобных решений может достигать 15-20 % [6, с. 5].

Идентификация по отпечаткам пальцев требует «остановки»: человек должен оказаться у сканера для проведения процедуры. Зато в таком случае и коэффициент ложного отклонения запроса (вероятность того, что система не признает подлинности отпечатка пальца зарегистрированного в ней лица) составляет не более 0,01 %. Тестирование отпечатков пальцев может подойти при открытии счета в банке или в процессе подтверждения финансовой транзакции. Со своей стороны, системы видеонаблюдения, позволяющие распознавать лица, пока больше применяются для опознания подозреваемых, чем при организации доступа в защищенные помещения.

Компании, планирующие использовать биометрию, должны понимать, что биометрическая аутентификация – это процесс, основанный на вероятностном подходе, а не на упрощенной системе приема / отказа.

Биометрической системы, которая всегда давала бы достоверные результаты, пока не создано. Так что организации должны сами искать баланс между коэффициентами приема и отказа, который соответствовал бы их потребностям, понимая, что повышение коэффициентов приема может привести к повышению вероятности ложного результата.

Критериями для достижения баланса станут целевые коэффициенты приема и отказа, установленные самой организацией в зависимости от технологий, которые она использует (уровня значимости операции или бизнес-процесса), а также других доступных методов аутентификации. Так что при управлении системой биометрической идентификации нужно руководствоваться спецификой соответствующего бизнес-процесса.

Необходимо также обеспечить безопасность биометрических сведений. Любой биометрический метод основан на сравнении шаблона или информации (ключа) с базой данных. На всю подобную информацию, скорее всего, будут распространяться правила, установленные в отношении персональных данных. Следовательно, придется следовать жестким требованиям в части использования, сбора и хранения таких сведений.

Компаниям придется предпринимать дополнительные меры предосторожности, чтобы в максимальной степени защитить данные от возможного

перехвата и незаконных манипуляций. После аутентификации биометрическая информация должна удаляться, если в ней больше нет необходимости.

Кроме того, организация, планирующая ввести биометрическую систему, должна обратить особое внимание на процесс регистрации. Вся цепочка биометрической аутентификации будет надежна только при условии, что процесс регистрации хорошо продуман.

Выводы

Развитие биометрии открывает новые возможности для многих компаний, рынков и отраслей, ее использование способно повысить точность идентификации клиентов, упростить процедуры проверки и верификации персональных данных для предоставления доступа к услугам, а также усилить безопасность наиболее важных процессов и бизнес-систем.

Во всем мире основным заказчиком систем биометрической идентификации традиционно выступало государство, в особенности силовые ведомства. В последнее время эти технологии подешевели – и теперь ждут массового применения в гражданском секторе в виде удобных систем контроля и управления доступом.

Таким образом, обычный бизнес все больше тяготеет к интеллектуальным инструментам управления информацией и сотрудниками.

Список литературы:

1. Аржанова Я. Тело-видение // Бизнес журнал. – 2013. – № 4. – С. 44.
2. Биометрия как инвестиция в бизнес [Электронный ресурс]. – Режим доступа: <http://indeed-id.ru/blog/?p=983> (дата обращения: 20.10.13).
3. Биометрия помогает банкам улучшить обслуживание клиентов [Электронный ресурс]. – Режим доступа: <http://newsland.com/news/detail/id/92093> (дата обращения: 22.10.13).
4. Золотов Е. В человеческом измерении // Бизнес журнал. – 2013. – № 4.
5. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. – СПб.: Политехника, 2001.
6. Стивен Дэвис, Шеймус Рейли. Пришло время использовать биометрические технологии в бизнесе. – 2013.
7. Ульянова Н. Открой личико! // Бизнес журнал. – 2013. – № 4. – С. 48.
8. Югринова Н. Верьте на слово! // Бизнес журнал. – 2013. – № 4. – С. 40.