

Безопасность на кончиках пальцев

Технологии защиты с помощью биометрической идентификации обещают стать прибыльным рыночным сегментом для реселлеров. В своей статье Гарет Кершоу (Gareth Kershaw) попытается выяснить, насколько эти технологии готовы к появлению на массовом рынке.

СП» (Продолжение. Начало на с. 1)

Сомнения у многих вызывает также надежность идентификационных систем. Используемые сейчас технологии сканирования отпечатков пальцев и радужной оболочки глаз обладают достаточно высокой погрешностью. Что касается систем распознавания лица, то они все еще находятся в стадии развития. Кроме того, на их работоспособность заметно влияют условия освещенности и некоторые другие факторы.

Оценивая размеры рынка систем биоидентификации, аналитики не могут прийти к единому мнению. Если не так давно IDC заявляла, что его оборот в 2005 году достигнет \$887 млн, то по прогнозам Frost & Sullivan, уже в 2006 году этот показатель превысит \$2 млрд. А исследователи International Biometrics Group уверяют, что в 2007 году продажи в данной сфере имеют все шансы достичь \$4 млрд.

Некоторые обозреватели, в частности Стив Эдейр (Steve Adair), мене-

джер Lenovo по продвижению ноутбуков ThinkPad на британском рынке, считают, что к существующим сегодня биометрическим технологиям следует относиться вполне серьезно. Ссылаясь на отчет Gartner, в котором сообщается, что к 2007 году 80 % компаний будут нуждаться в усилении систем аутентификации с помощью альтернативных методов проверки, г-н Эдейр убежден в жизнеспособности технологии идентификации по отпечаткам пальцев. Другие же, наоборот, уверены, что массовый рынок завоюют новые системы биометрической идентификации, которые появятся в будущем.

В ситуациях, когда высокого уровня безопасности не требуется, надежность, обеспечиваемая системами распознавания отпечатков пальцев, вполне приемлема. Однако такие системы не годятся для обеспечения доступа нескольким пользователям. В этом случае вероятность получения отказа может быть высокой – и не в последнюю очередь из-за загрязнения самого датчика вследствие частого физического контакта, считает Майк Нелсон (Mike Nelson), вице-президент Fujitsu Europe по региону EMEA.

Тем не менее г-н Нелсон не сомневается в неизбежности повсеместного использования технологий биометрической идентификации. Они больше не являются чем-то из области



Гэри Дьюк, руководитель консультационного центра компании LAN 2 LAN: «Компании должны получить легко управляемое целостное решение, а не отдельные продукты»

фантастики – технологии работают, и их достаточно просто внедрять. Биометрия активно применяется во многих отраслях, особенно в системах безопасности авиаперевозок и банковской сфере. А ее массовое внедрение в повседневную жизнь является лишь вопросом времени, считает Майк Нелсон.

Глава департамента Siemens Communications по системам иденти-

фикации Колин Роббинс (Colin Robbins) согласен с утверждением Нелсона, но добавил, что требуется рассматривать биометрию как нечто большее, чем средство безопасности. Сегодня биометрические системы позиционируются исключительно как механизм защиты доступа к помещению, компьютерам или сети. Однако если искусственно ограничить спектр их применения только вышеперечисленными областями, то затраты могут показаться неоправданно высокими.

Другими словами, средства биометрического контроля должны не просто защищать, но и обеспечивать доступ к определенному набору бизнес-функций. Такое возможно, если биометрический механизм рассматривается в качестве составной части всей системы управления идентификацией. Это позволяет совершать онлайн-новые платежи или внедрять электронные бизнес-процессы, требующие повышенного уровня безопасности, считает Колин Роббинс.

По мнению Гэри Дьюка (Gary Duke), руководителя консультационного центра по сетевому администрированию компании LAN 2 LAN, хотя число биометрических продуктов на рынке с каждым днем увеличивается, компаниям нужно нечто большее. Они должны получить легко управляемое целостное решение, а не просто отдельные продукты.

Потенциально такие предложения могут появиться в нескольких областях. Существующие технологии – включая те, которым так и не удалось попасть на массовый рынок из-за сложностей с интеграцией – все же имеют возможность достичь зрелости, если станут более совершенными.

По утверждению Бори Тоф (Bori Toth), отвечающей за биометрические проекты в Deloitte & Touche, распознавание личности по радужной оболочке глаза является одной из таких областей. Системы, использующие данный принцип, считает г-жа Тоф, обладают достаточной точностью, скоростью работы, защитой от злоумышленников и удобством использования. Скептицизм по поводу этой технологии большей частью вызван ее относительной молодостью. Одних смущает то, что световой диапазон, который используют подобные системы, близок к инфракрасному, других – то, что по снимкам радужной оболочки глаза, как уверяют иридологи, можно узнать о состоянии здоровья человека. Ни одно из этих опасений не имеет под собой научной основы, отметила г-жа Тоф.

БУДУЩЕЕ – ЗА СИСТЕМАМИ КОМБИНИРОВАННОЙ ИДЕНТИФИКАЦИИ



Александр Колпаков, директор департамента систем безопасности корпорации «Инком»

сфера очень высокотехнологична. Здесь требуется слаженная работа как специалистов в области безопасности, так и ИТ-профессионалов.

Еще одна проблема – очень размытые представления у заказчиков о том, чего именно они хотят от биометрического контроля. Поступали, к примеру, такие заказы – реализовать доступ на завод с проверкой по отпечаткам пальцев, чтобы рабочие не могли обмениваться пропусками. В данном случае заказчик не учел того, что сама по себе биометрическая идентификация имеет еще некоторые технические ограничения: эти процедуры не быстрые, поэтому нужно внимательно анализировать, где системы биометрии можно применять, а где – нет.

В Украине наиболее часто к биометрическому контролю прибегают в банковском сегменте. Востребованы системы идентификации по отпечаткам рук, пальцев. Сейчас уже

активно применяется идентификация по лицу. Помимо банков системы биометрии используют на специализированных производствах, где требуется ограничить доступ в определенные зоны.

Если говорить о технической стороне вопроса, то комбинированные технологии идентификации, когда она осуществляется по ряду параметров (к примеру, вес человека и отпечатки пальцев), намного перспективнее отдельных решений.

Что касается, например, безопасности сети, то до недавнего времени речь шла в основном только о защите ее периметра. Однако до настоящего времени 95 % всех сетей остаются незащищенными изнутри. Значит, до рабочего места безопасность так и не доходит. Если говорить о тенденции, то сейчас идет активное движение в сторону надежной биометрической идентификации пользователя на рабочем месте.

Сегодня украинский рынок систем биометрической идентификации личности развит недостаточно, и тому есть несколько причин. Одна из них связана с тем, что данная

ОСНОВНАЯ ПРОБЛЕМА РЫНКА БИОМЕТРИИ – СТЕРЕОТИПЫ



Виктор Сарбаш,
директор компании «Сарбаш Лаб»

Украинский рынок биометрической идентификации только начинает формироваться. Полтора года назад, когда мы только начинали, такие сенсоры внедрялись в основном на небольших объектах (до 50 человек), например в банках. Теперь же биометрические систе-

Еще одна технология – идентификация по голосу. Такие системы создает, например, компания 192.com Business Services. По словам ее ИТ-директора Пола Брума (Paul Broome), несмотря на то что идентификация по голосу все еще пребывает на стадии разработки, она идеально подходит для решения таких задач, как, например, онлайн-новая аутентификация.

Однако прежде чем эта или любая другая биометрическая технология сможет приносить весомую прибыль, придется преодолеть ряд трудностей. Фрэзер Томас (Fraser Thomas), CEO Swivel Secure, отметил, что на сегодняшний день основными преградами к тотальному развертыванию биометрических систем являются вопросы цены, внедрения и неприкосновенности права на личную информацию.

Еще одним ключевым моментом, по мнению Колина Роббинса, является общественное мнение. Чтобы технология имела успех, она должна рассматриваться конечными пользователями как средство, способное облегчить их жизнь (например, вместо того чтобы помнить множество паролей, пользователь аутентифицирует себя всего один раз).

Для этого компании и их поставщики должны сосредоточиться не на конкретной биометрической системе, а на возможностях, предоставляемых ею для бизнеса.

Как утверждает Колин Роббинс, биометрическая система контроля сама по себе мало что значит, если существует вероятность ошибочного

мы контроля доступа (СКД) часто устанавливают на проходных крупных промышленных предприятий.

На сегодняшний день самый распространенный в мире тип системы биоидентификации – это идентификация по отпечатку пальца. Хотя мы в первую очередь производители (разработчики), нам приходится заниматься также установкой и интеграцией. И в ближайшие 1–2 года мы продолжим выполнять эти функции, так как новую, а тем более биометрическую, систему достаточно сложно вывести на рынок: необходимо провести много инсталляций на крупных объектах. Тем не менее шаги по формированию партнерской сети делаются уже сейчас.

Основная проблема, с которой мы сталкиваемся, – это сложившиеся стереотипы. Первое время было тяжело объяснить людям, что технология управления доступом в помещения по отпечаткам пальцев – уже не миф, а реальность украинского рынка.

срабатывания или взлома. Неверно работающий механизм идентификации может быть даже хуже, чем его полное отсутствие.

Также очень важен вопрос соотношения цены и производительности. Внедрение механизмов биометрического контроля может оказаться слишком дорогостоящим делом, если рассматривать их отдельно от всей бизнес-системы.

По словам г-на Дьюка, ситуация постепенно улучшается: «Вопрос цены является одной из основных проблем в данной области. Однако с каждым днем биометрические решения становятся все более доступными».



Майк Нелсон, вице-президент Fujitsu Europe по региону EMEA:
«Знание потребностей пользователей и построение эффективной системы взаимоотношений с ними – ключ к успеху»

Бори Тоф согласилась с мнением г-на Дьюка, заявив, что нигде за последние годы не наблюдалось такого падения цен, как в сегменте сканеров радужной оболочки глаза. А реализация масштабных биометрических проектов приведет к дальнейшему удешевлению этих устройств.

Однако смогут ли механизмы биометрической идентификации стать основным средством корпоративной защиты? Майк Нелсон, например, уверен, что биосистемы необходимо совмещать со стандартными механизмами идентификации – смарт-картами или PIN-кодами.

Несмотря на все недочеты биометрические технологии, похоже, отвечают основному требованию, предъявляемому к системам персональной идентификации. Пароли легко забыть. Они также могут быть украдены или взломаны. Магнитные карты и традиционные удостоверения личности (например паспорта) легко подделать. Однако, по утверждению г-жи Тоф, благодаря биометрии решение данных проблем не за горами. Возможно, качественные изменения произойдут уже в следующие несколько лет. Биометрия – не панацея. Тем не менее это большой шаг вперед. Биометрические технологии способны связать информацию с конкретным человеком, что не позволяет ни один из традиционных методов.

Бори Тоф признает, что глобальное внедрение таких систем займет какое-то время. На первом этапе далеко не каждому потребуются установка биометрических сенсоров. На протяжении нескольких лет подобные устройства будут предлагаться в качестве дополнительной опции к уже существующим продуктам.

Такой последовательный переход обеспечит реселлерам и системным интеграторам огромное поле для деятельности, поскольку внедрение биометрических систем требует глубоких знаний бизнес-процессов и высокой квалификации в сфере безопасности.

«Реселлеры должны пристально наблюдать за последними разработками в данной области. Знание нужд пользователей и построение эффективной системы взаимоотношений с ними – ключ к успеху», – утверждает Нелсон.

Джеки Грувс (Jackie Grooves), главный менеджер отдела безопасности Utimaco Safeware, считает, что каждый участник канала продаж должен избрать ту область биометрии, которую ему по силам продвигать. Так, если реселлер специализируется на сетевых технологиях, то, возможно, средства сетевой безопасности станут наиболее прибыльным для него сегментом. Если же основной сферой деятельности являются веб-технологии, то бизнес нужно нацелить на системы обеспечения безопасности транзакций.

CP > Инфокод 603089

МИРОВОЙ РЫНОК БИОМЕТРИИ

● На мировом рынке биометрические системы идентификации и безопасности выходят на пик популярности. Особо отмечают в этом сегменте рынка японские производители, которые активизировались на фоне растущего числа киберпреступлений и случаев мошенничества, связанных с кредитными картами и банковскими транзакциями. Компания Yano Research Institute обнародовала информацию о том, что объем американского рынка биометрических систем контроля по итогам 2004 года достиг \$79,5 млн, что на 39 % больше, чем два года назад. По прогнозам аналитиков, к 2010 году отрасль разрастется до \$245 млн, это связывается с адаптацией биометрических систем идентификации под мобильные телефоны и портативные компьютеры.

● Растущий интерес к биометрическим системам способствовал и тому, что эта отрасль на мировом рынке стала активно развиваться. По предварительным прогнозам, к 2008 году объем рынка достигнет \$4,6 млрд. В 2003 году эта цифра составляла \$719 млн.

● На сегодняшний день ведущими поставщиками биометрических систем безопасности и идентификации являются Alcatel, Nuance Communications и SAFLINK. Их продукция представлена программным обеспечением для опознавания личности по таким уникальным признакам, как отпечатки пальцев, сетка вен на ладони и лицо. Среди японских разработчиков особо отмечается компания Fujitsu Frontech, имеющая огромный потенциал, а также компания T.D.I., которая начинает активное продвижение биометрических систем для идентификации человека по внешности. Представители компании рассчитывают, что их разработка заинтересует производителей входных дверей и замков.

● Некоторые крупные организации уже активно используют биометрические системы для осуществления более эффективного контроля. Второй по величине японский банк Mitsubishi Tokyo Financial Group в минувшем году уже ввел в обращение биометрический контроль в сети своих банкоматов. А Japan Post в нынешнем году планирует ввести в обращение пластиковые карты с поддержкой идентификации клиентов по сетке капилляров на пальцах.