Биометрия. От идентификации личности к идентификации мыслей.

Существует несколько особенностей, которые отличают российские компании, работающие на рынке высоких технологий, например, в области биометрии. Прежде всего, это значительный проигрыш в капитале и оборотных средствах по сравнению с ведущими зарубежными компаниями – конкурентами. Отсутствие реального биометрического рынка в России и отсутствие интереса у государства также не упрощает жизнь российским компаниям, претендующим на реальные достижения в области high tech. Последней напастью явилось резкое снижение общей активности на мировом рынке венчурного капитала и падение интереса к высокотехнологическим компаниям в частности. Для российских компаний единственной возможностью выжить в таких условиях остается правильное определение стратегических направлений развития биометрических технологий на 10 – 15 лет вперед, что может позволить компании оставаться конкурентоспособной в своих разработках, затрачивая при этом в сотни раз меньше средств, чем зарубежные фирмы.

Правильный прогноз на будущее невозможен без детального анализа прошлого. Биометрические системы в настоящее время представляют собой второе поколение систем безопасности, а биометрия считается наукой, использующей измеряемые уникальные параметры человека для его идентификации. Современная биометрия насчитывает не более десяти лет, хотя ещё более 5 тысяч лет назад люди использовали для идентификации отпечатки пальцев. Современная биометрия также появилась из дактилоскопии, когда в дополнение к громоздким полицейским AFIS появились технические средства – дактилоскопические сканеры, а возможности

вычислительной техники позволили осуществлять идентификацию пользователя в режиме реального времени. До появления биометрических систем идентификация пользователя или вход в систему (на объект) осуществлялась только с помощью постоянных величин, таких как обыкновенный механический ключ или персональный номер (PIN) – число, которое может храниться на любом носителе в открытом или закодированном виде. Принципиальным признаком систем безопасности первого поколения является однозначность и/или постоянство во времени и пространстве идентификационного параметра, в то время как биометрический параметр пользователя, также принципиально, всегда является переменной величиной, зависящей от множества факторов. При этом задача правильной идентификации для биометрических параметров значительно сложнее, чем идентификация постоянных параметров для систем первого поколения. С информационной точки зрения системы биометрической идентификации представляют собой второе поколение систем безопасности, осуществляющих идентификацию пользователя, используя переменную величину.

Проследим прогресс и проанализируем факторы, повлиявшие на развитие биометрии за последние 10 лет. Существенно увеличилось количество различных биометрических параметров, используемых для идентификации. Идентификация по голосу, лицу, руке, глазу в сумме превосходит классические системы идентификации по отпечатку пальца, которые, в свою очередь, используют различные принципы для получения дактилоскопического изображения, а именно: оптические сканеры, работающие на эффекте полного внутреннего отражения света (можно сказать, что с них и началась современная биометрия!), емкостные CMOS чипы, волоконно-оптические чипы и теплорегистрирующие чипы. Увеличилось и число компаний, занимающихся биометрией, и приблизилось к 400. Соответственно

увеличилось и количество областей, в которых биометрические системы находят реальное применение, из которых, безусловно, наиболее массовыми являются мобильная связь, паспортные системы и кредитные карты (безналичные расчеты). Крупные биометрические компании, занимающиеся разными областями биометрии, заключают союзы и объединяются, как например Vision & Identix с общим количеством акций 600 млн. USD [www.identix.com].

Несмотря на то, что общий рынок биометрических систем устойчиво увеличивается в последние несколько лет, примерно на 40% в год [www.biometricgroup.com] (это очень высокие темпы роста относительно других направлений high tech), его развитие происходит достаточно своеобразно. Например, несколько компаний [Harris, Siemens] ещё в 1998 году анонсировали выпуск мобильных телефонов, обеспечивающих защиту аппарата при включении отпечатком пальца пользователя (вместо PIN). Однако до настоящего времени такие телефоны не появились в продаже, хотя функция распознавания слов и пользователя по голосу реализована уже во многих моделях мобильных телефонов и встроенные в трубку телевизионные камеры также перестают быть экзотикой.

События 11 сентября значительно изменили отношение к биометрии в мире. На данный момент известно, что 11 террористов – организаторов атаки на США были известны ФБР и разыскивались властями США, однако использование террористами поддельных документов и бюрократический механизм регистрации иностранцев сделали возможным осуществление теракта. Кроме того, отсутствие биометрической защиты при управлении самолетом также не препятствовало осуществлению планов террористов, хотя использование простого дактилоскопического сканера, блокирующего передачу управления самолета другому лицу, могло существенно уменьшить последствия террористической атаки.

Все это способствовало увеличению популярности глобальных биометрических решений среди граждан США, всего 10 % которых поддерживало идею биометрической паспортизации до 11 сентября 2001 года и более 75 % после. Однако наличие множества различных решений биометрической паспортизации и лоббирование несколькими крупными компаниями свих подходов для решения этой проблемы на паспортном рынке (IBM, Polaroid, Oracle, Microsoft) затрудняет принятие единого решения, а многочисленные локальные биометрические системы несовместимы по параметрам и скорее препятствуют созданию глобальной биометрической сети, чем способствуют её созданию.

Аналогичная ситуация существует и в области биометрической защиты кредитных карт, только в роли независимых государств и служб выступают крупнейшие карточные компании Visa, MasterCard, American Express, их филиалы и отдельные банки. Однако, если термин "угроза международного терроризма" является наиболее популярной фразой в устах современных государственных деятелей, то банки и финансовые компании, прежде всего, заинтересованы в снижении своих расходов, в получении максимальной прибыли и не готовы к осуществлению относительно дорогостоящих биометрических решений. Поэтому, не смотря на то что технически банковская сфера готова для введения биометрической защиты кредитных карт, никто не хочет брать на себя дополнительные затраты по биометрической защите, а предпочитают скрывать потери от несанкционированного доступа, составляющие в целом сотни миллионов USD в год [www.identitytheft.org].

Таким образом, получается что, несмотря на техническую готовность, в ближайшее время не стоит ожидать широкого захвата указанных массовых применений биометрическими решениями. Однако более дальний прогноз не

вызывает особых сомнений относительно биометрической паспортизации населения. Тенденция политического развития такова, что биометрическая паспортизация может быть практически единственной защитой как для развитых государств, так и отдельных граждан от преступности и терроризма, а многочисленные участившиеся военные конфликты начала XXI века могут только ускорить принятие совместного межгосударственного решения. Вероятно, останутся страны, которые не присоединятся к системе единой паспортизации (например, страны из "оси зла" или которые не будут способны участвовать в этом решении, исходя из технико-экономических соображений), однако это приведет только к большей изоляции неприсоединившихся государств и их граждан от цивилизованного мира. Ориентировочно население Земли к 2010 году достигнет 10 млрд. человек, что при минимальной стоимости биометрического удостоверения в 1 USD ограничивает минимальную емкость рынка только удостоверений величиной 10 млрд. USD. Реальная величина этого рынка будет значительно больше и конечно представляет существенный интерес для компаний любого уровня.

Расширение измеряемых и анализируемых биометрических параметров приводит к естественному расширению круга вопросов, решаемых биометрией. Другим наиболее перспективным направлением биометрии является анализ психофизиологического состояния человека, известный большинству читателей по термину "детектор лжи". Определение истинных мыслей и целей человека задача не менее древняя, чем его идентификация. Она решалась различными доступными техническими средствами, например длительными пытками во времена инквизиции или допросами с применением полиграфа. Одним из основных принципов психофизиологических детекторов является зависимость между количеством получаемой от испытуемого информации и временем тестирования. Естественно,

что для получения достоверного результата надо увеличивать или время тестирования, или эффективность считывания биометрической информации. Для классических полиграфов (детекторов лжи) используется измерение нескольких биометрических параметров (обычно пульс, ЭКГ, кожно-гальваническая реакция), имеющих производительность примерно 100 – 200 отсчетов в секунду, при этом время тестирования составляет несколько часов [www.polygraph.com]. Использование многоканальной электроэнцефалограммы позволяет повысить производительность получения информации до 1000 отсчетов в секунду и понизить время тестирования до получаса [www.brainwavescience.com]. Применение голосовых детекторов лжи позволяет добиться времени тестирования в несколько минут при производительности порядка 10 тысяч отсчетов в секунду [www.catchcheater.com]. Прогресс, безусловно, налицо, однако, как и в случае идентификации, для реализации массовых применений необходимо ограничить время тестирования несколькими секундами, что вероятно и будет достигнуто в течение ближайших десяти лет.

Итак, какие глобальные изменения ожидают мир в 2010 – 2020 годы, по прогнозу автора.

1. Практически все население земли будет иметь биометрические удостоверения личности, информация о которых хранится в государственных базах данных, объединенных в глобальную международную идентификационную систему.

2. Реальностью станет не только идентификация личности, но и идентификация мыслей и намерений. При пересечении границ государства или при доступе на определенные объекты человек будет проходить автоматическое психофизиологическое тестирование в течение реального времени (не более 10 секунд) на предмет представления опасности для этого государства или объекта.

Таким образом, государства могут защищаться не только от известных преступников, но и от людей, ранее не совершавших преступлений, но имеющих преступные намерения. В данный момент решение подобной задачи особенно актуально для Израиля, граждане которого подвергаются постоянным атакам шахидов – самоубийц, хотя, как показали события 11 сентября, ни одно государство в мире не застраховано от возможных атак террористов.

В заключение, вернемся к ситуации на биометрическом рынке в России. К сожалению, несмотря на наличии высококвалифицированных технических специалистов, в силу объективных причин, изложенных в начале статьи, в настоящее время в России совсем немного компаний, профессионально занимающихся биометрией и отстаивающих самостоятельные идеи и решения в области биометрии. Возможно некоторое улучшение ситуации после образования 14 марта 2002 года "Русского биометрического общества". Однако, в настоящее время только 4 российские компании из общего количества 389 (!) оказались включены в международную Биометрическую Информационную директорию (BID), а именно: BioLink [www.biolink.ru], Speech Technology Center (речевые технологии) [www.speechpro.ru], Sonda (AFIS) [www.sonda.ru] и Elsys [www.elsys.ru]. Компания BioLink, которая хоть условно, но может быть названа российской, первая выпустила на рынок компьютерную мышь со встроенным дактилоскопическим сенсором (1999 год) и успешно развивает сетевые решения на базе своих дактилоскопических сенсоров.

Компания "Элсис" также первая в мире предложила на рынок чиповое решение для дактилоскопических систем на базе волоконно-оптического чипа собственной разработки (DactoChip, 1995).

Разработанное "Элсис" биометрическое удостоверение личности BiCard и оригинальная система считывания удостоверения и живого пальца пользователя одним сенсором (чипом) может быть основой национальных или глобальных паспортных систем. В 1999 году компания победила своих гораздо более именитых конкурентов в тендере на реализацию биометрического паспорта Вьетнама (75 млн. населения).

Новые биометрические технологии, разрабатываемые компанией "Элсис": объемный пульс (3D-pulse) и виброизображение (VibroImage) позволяют получать более 10 млн. информативных отсчетов в секунду о психофизиологическом состоянии человека и могут быть использованы для построения биометрических систем третьего поколения, одновременно в течение 10 секунд осуществляющих идентификацию личности и тестирование мыслей пользователя.

К сожалению, велика вероятность того, что идеи, задуманные российскими учеными, будут реализованы другими компаниями, как это уже произошло с чиповой дактилоскопией, т.к. для защиты и продвижения своих решений необходимы значительные вложения, которыми не обладают российские биометрические компании, а государственной помощи также не ожидается для решения, в общем-то, государственных задач.

Заключение.

Упреки президента РФ В.В.Путина в недостаточной амбициозности планов, адресованные российскому правительству, следует переадресовать и большинству российских компаний, занимающихся биометрией. Практически все, даже начинающие американские компании (не говоря уже о крупных) ставят своей целью полный или ощутимый захват мирового рынка, в то время как российские компании

пытаются решать свои мелкие локальные задачи. Для нормального роста российской экономики необходима не только реальная поддержка сверху, но и активная деятельность и агрессивные планы российских компаний, работающих в области высоких технологий.

Данную статью следует прочитать и российским капиталистам и финансистам. Возможно, через 10 – 15 лет будет также выгодно иметь акции биометрических компаний, как сегодня выгодно иметь акции Intel или Microsoft.

Виктор Минкин

Заместитель директора Многопрофильного Предприятия "Элсис"

Вице-президент Русского Биометрического Общества

minkin@elsys.ru