А.Иванов, А.Малыгин

ВЫСОКОНАДЕЖНАЯ БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ:

ПОСЛЕДНИЙ ДЮЙМ ПЕРВОЙ МИЛИ

"И он сделал то, что всем – малым и великим, богатым и нищим, свободным и рабам – положено будет начертание на правую руку или на чело их,

И что никому нельзя будет ни покупать, ни продавать, кроме того, кто имеет это начертание, или имя зверя, или число имени его".

Откровение Святого Иоанна Богослова, гл.13, ст. 16–17

Аутентификация пользователей в различных системах доступа становится все актуальней. Особенно важна эта проблема для открытых, массовых телекоммуникационных и информационных систем. Одно из наиболее перспективных направлений защиты подобных систем от несанкционированных воздействий – биометрические методы идентификации пользователей. Однако, несмотря на всю привлекательность, данный подход сопряжен с рядом серьезных проблем. В предлагаемой статье авторы анализируют уязвимость традиционных биометрических систем идентификации и рассказывают о новом подходе, основанном на динамических биометрических образах человека и методах нейросетевого анализа.

В последние десятилетия достижения науки и новейшие технологии как никогда прежде определяют динамику экономического роста, уровень благосостояния населения, конкурентоспособность государства в мировом сообществе, степень обеспечения его национальной безопасности и равноправной интеграции в мировую экономику. Стремительное развитие и широкое использование современных информационно-телекоммуникационных систем ознаменовали переход человечества от индустриального общества к обществу информационному, в основе которого лежат новейшие системы коммуникации. Количество, технический уровень и доступность информационных систем уже сейчас определяют степень развитости страны и ее статус в мировом сообществе, а в недалеком будущем, несомненно, станут решающим показателем этого статуса.

Вместе с тем, процесс информатизации мирового сообщества порождает комплекс негативных явлений. Действительно, высокая сложность и одновременно уязвимость всех систем, на которых базируются региональные, национальное и мировое информационные пространства, а также фундаментальная зависимость от их стабильности государственных инфраструктур приводят к возникновению принципиально новых угроз. Эти угрозы связаны, прежде всего, с потенциальной возможностью использовать

информационно-телекоммуникационные системы в целях, несовместимых с задачами поддержания международной стабильности и безопасности, уважения прав и свобод человека.

Поэтому все более актуальной становится проблема *аутентификации пользователей,* имеющих доступ к общественным и личным информационным ресурсам. Наиболее подходящей и получившей широкое распространение в последние годы технологией является *аутентификация личности по его биометрическим данным.* Одна из важнейших задач биометрии – создание технических устройств, способных узнавать конкретного человека по его неповторимым биометрическим характеристикам и с еще более высокой вероятностью распознавать злоумышленников, пытающихся маскироваться под легальных пользователей.

Сегодня признанным лидером разработки и внедрения биометрических технологий являются США. Толчком к бурному развитию таких технологий стали трагические события 11 сентября 2001 года, хотя начало исследований в данной области было положено еще в середине 1980-х годов. С целью поддержки программ по биометрии правительство США в 1995 году создало биометрический консорциум (www.biometrics.org), куда вошли государственные и частные организации, университеты, исследовательские центры, лаборатории тестирования и сертификации продуктов биометрических технологий. Сейчас в него входят примерно 500 различных организаций. Правительством США создан и Национальный биометрический тестовый центр при университете Сан-Хосе (www.engr.sjsu.edu/biometrics), в период с 1998 года по настоящее время организована подготовка специалистов по биометрии в пяти различных университетах страны. Национальные институты стандартизации США (NIST и ANSI) за последние 10 лет разработали порядка 40 национальных биометрических стандартов, большинство из которых в данный момент используется как основа при разработке международных биометрических стандартов специально созданным подкомитетом ISO/IEC JTC1 SC37.

Параллельно с государственным биометрическим консорциумом США при поддержке правительств ведущих стран образована Международная ассоциация производителей средств биометрии (International Biometric Industry Association, www.IBIA.org), куда входят 26 крупнейших производителей биометрических устройств. Правительство США в 1998 году поддержало и создание BioAPI Consortium для разработки промышленного стандарта интерфейсов связи (API) различных биометрических программно-аппаратных приложений.

Все вышеперечисленное свидетельствует о значительном внимании к развитию биометрических технологий. Усиление паролей и персональных кодов биометрией официально рассматривается Международной организацией по стандартизации ISO (в лице ее подкомитета SC37 по вопросам биометрии при первом объединенном комитете JTC1) как одна из основных тенденций развития систем информационной безопасности. После решения лидеров группы восьми ведущих стран в 2002 году встала задача унификации биометрических данных в национальных электронных паспортах разных стран. По сути, именно это обстоятельство и форсировало работу недавно созданного биометрического подкомитета ISO/IEC JTC1 SC37 (www.din.de/ni/sc37).

Производители биометрических устройств и технологий объединены в рамках международной ассоциации IBIA (International Biometric Industry Association), которая активно влияет на процессы подготовки новых стандартов. Через IBIA производители регистрируют свои форматы представления биометрических данных, которые далее гармонизируются и обобщаются в виде международных стандартов и рекомендаций. На данный момент зарегистрировано 27 форматов данных, используемых в биометрических устройствах и технологиях различных компаний.

Естественно, что Россия не может оставаться в стороне от наметившихся процессов объединения международных усилий и стандартизации биометрических технологий. В лице Госстандарта РФ выступает полноправным членом ISO/IEC. В феврале 2003 года при ГОСТ Р ТК355 (технический комитет "Автоматическая идентификация") был создан 7-й подкомитет, занимающийся только вопросами биометрической идентификации. На ГОСТ Р ТК355/ПК7 возлагается работа по переводу международных биометрических стандартов на русский язык и их гармонизации.

Стандарты, разработанные ISO/IEC JTC1 SC37, принадлежат к относительно *"слабой биометрии"*, способной выполнить полицейские функции и идентифицировать личность человека только локально, под прямым контролем проверяющего. Последний (например, пограничник) обязательно должен контролировать действия проверяемого в ходе процедуры автоматизированной биометрической идентификации. Присутствие проверяющего гарантирует, что предъявлен образ именно контролируемого человека, а не физический муляж.

ОБ АВТОРАХ

Иванов Александр Иванович – начальник лаборатории нейросетевых и биометрических технологий ФГУП "Пензенский электротехнический институт"

Малыгин Александр Юрьевич – начальник межведомственной лаборатории тестирования биометрических устройств и технологий Пензенского государственного университета

E-mail: mal@stup.ac.ru

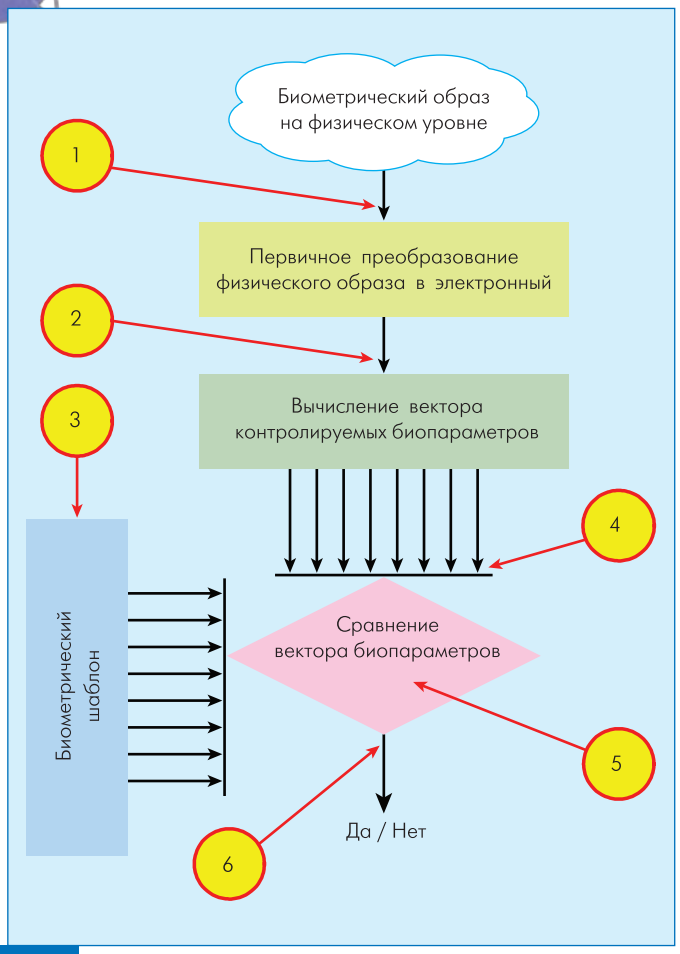

Рис.1 Точки типовых атак в системе биометрической идентификации, выполненной с классическим решающим правилом Да/Нет

Большинство существующих технологий используют статические (неизменяемые по воле человека и данные ему от рождения) биометрические образы [1, 2]. К ним относятся аутентификация по:

- рисунку радужной оболочки глаза;
- рисунку кожи кончиков пальцев (по узору папиллярных линий;
- 2D- и 3D-параметрам геометрии кисти руки и лица человека;
- рисунку кровеносных сосудов: глазного дна, глазного яблока, тыльной стороны кисти руки;
- геометрии ушных раковин;
- электрокардиограмме сердца;
- запаху тела;
- генотипу;
- ионному спектру следов пота.

Для аутентификации *мобильных пользователей* в открытом информационном пространстве все перечисленные методы оказываются малоэффективны. Основная причина этого – в высокой уязвимости биометрической защиты, построенной на статических биометрических образах. На рис.1 приведена блок-схема типовой биометрической защиты, основанной на статической биометрии и классическом решающем правиле. Такая система защиты подвержена ряду типовых атак, точки реализации которых на рис.1 помечены цифрами.

Точка 1 представляет собой окно датчика системы защиты. Предположим, что это – окно сканера отпечатка пальца. Очевидно, что злоумышленник, находящийся перед окном сканера, может реализовать несколько типовых атак:

- атака случайного подбора (предъявляется несколько образцов рисунков в надежде обнаружить коллизию совпадения параметров зарегистрированного и предъявленного рисунков);
- атака компрометации предшествующего рисунка (с поверхности сканера снимается отпечаток пальца человека, только что прошедшего положительную идентификацию);
- атака на анонимность легальных пользователей (выясняется имя, адрес, иные данные легального пользователя биометрической защиты для последующей реализации атаки компрометации);
- атака предъявления муляжа (после реализации атаки компрометации биометрического образа изготовливается его муляж, который и предъявляется системе защиты).

Точки 2–6 открыты для атак в том случае, если у злоумышленника есть доступ к программному обеспечению того или иного средства биометрической защиты. Эта ситуация характерна для средств биометрической защиты информации (например, защиты доступа к информации). Защищая свою информацию на компьютере, работающем под широко используемой операционной системой, никто не может гарантировать отсутствие в вычислительной среде новой программы-шпиона и нового вируса.

Основная атака в **точке 2** – атака перехвата (компрометации) электронного биометрического образа пользователя. Злоумышленникам много выгоднее иметь электронный вариант реальных биометрических образов пользователя, чем физический муляж. Время на изготовление такого муляжа может занимать несколько часов. Технически невозможно изготовить сотни тысяч и миллионы физических муляжей, для электронных муляжей это не трудно. Как следствие, преступные сообщества будут стараться похитить базы реальных биометрических образов и незаконно собирать биометрию добропорядочных граждан с целью последующей организации атак подбора. Естественно, что биометрические базы образов преступными сообществами будут формироваться и применяться в электронной форме. То есть в точке 2 возможны три типа атак:

- атака компрометации электронного биометрического образа;
- атака случайного подбора электронного образа или перебора заранее заготовленной базы электронных биометрических образов;
- атака подстановки ранее скомпрометированного биометрического образа легального пользователя.

Точкой 3 атаки на биометрическую защиту является биометрический шаблон. Очевидно, что достаточно подменить биометрический шаблон легального пользователя на шаблон злоумышленника и система биометрической защиты пере-

станет выполнять свою основную функцию. В этой точке возможны два типа атак:

- атака компрометации биометрии для незаконного формирования баз реальных биометрических образов;
- атака подмены биометрии реальных пользователей на биометрию злоумышленников.

Наиболее уязвимым в биометрической защите является классическое решающее правило. Его можно атаковать с трех точек: с входа (точка 4), с выхода (точка 6), также может быть атаковано само тело решающего правила (точка 5).

В **точке 4** могут быть реализованы:

- атака компрометации вектора биометрических параметров;
- атака подмены вектора биометрических параметров на ранее перехваченный;
- атака случайного подбора.

В **точке 5** может быть реализована атака искажения приемлемых допусков решающего правила. Достаточно в несколько раз расширить допуска решающего правила, чтобы сделать биометрическую защиту практически бесполезной. Как "своего" она будет воспринимать любого.

Наиболее распространенной является атака, реализуемая в **точке 6** на "последний бит" решающего правила. Если в программе защиты найден "последний бит" решающего правила, то достаточно его изменить – и защита будет снята. Возможность тиражирования средств автоматического взлома является существенной угрозой для классической биометрической защиты. Бессмысленно исследовать новую программу для того, чтобы атаковать только одного человека. Иное дело, когда эффект удачной атаки удается тиражировать. Хакер, исследующий программу защиты, фактически надеется на возможность тиражирования результатов своего исследования, только в этом случае затраты окупаются.

Приведенный выше перечень уязвимостей и возможных атак на статическую биометрическую защиту с классическим решающим правилом порождает ряд проблем, которые необходимо решать. Это такие проблемы, как

- незаконный массовый сбор биометрических данных преступными сообществами;
- безопасность хранения биометрических данных в системах и устройствах;
- атаки на коллизии слабой биометрии;
- синтез физических и электронных муляжей и обмана биометрии с их использованием;
- обеспечение анонимности биометрии;
- ликвидация последствий компрометации статических, неизменяемых биометрических образов;
- индивидуальное тестирование обученных узнавать конкретного человека средств биометрии.

Всю группу перечисленных выше проблем для биометрии статических, неизменяемых образов одновременно решить не удается. Это делает применение подобных технологий для защиты персональной информации бесперспективным.

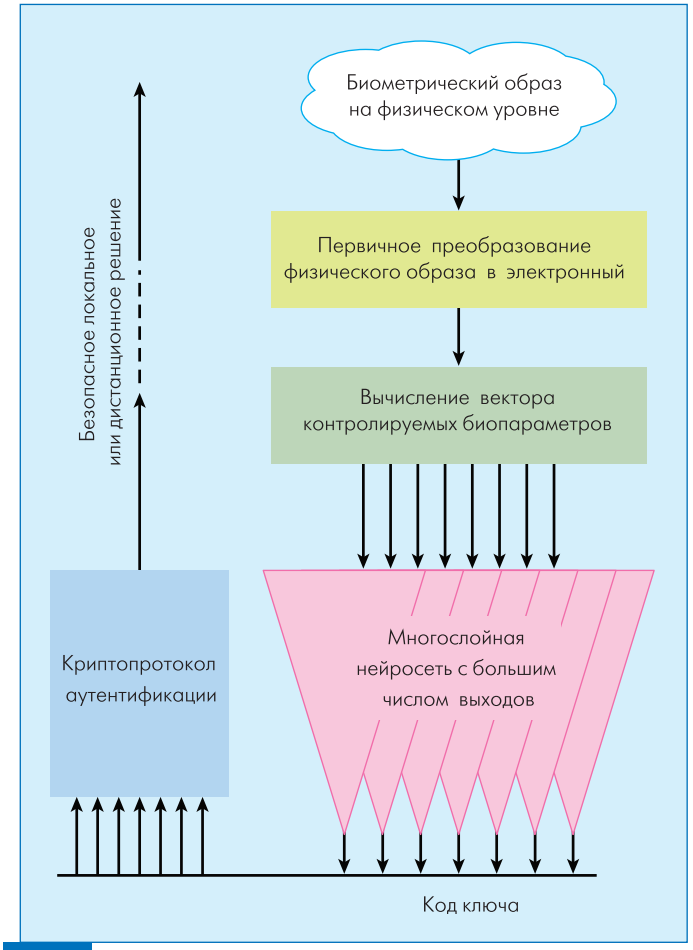

Рис.2 Процедуры биометрической аутентификации, выполненные с нейросетевым преобразованием биометрии в ключ

Иными словами, эти технологии будут широко применяться в государственных и корпоративных системах, где обязателен дополнительный контроль специальных служб.

Для аутентификации же мобильного пользователя ожидать широкого распространения подобных технологий, видимо, не следует. Свой криптографический ключ нельзя связывать со своим отпечатком пальца, так как мы оставляем свои отпечатки пальцев где угодно (оставлять где угодно свой ключ или пароль нельзя). Рано или поздно все наши отпечатки пальцев окажутся в одной из баз, незаконно сформированных преступным сообществом. Это вполне реальная угроза, причем она куда более реальна и близка, чем угроза "печати зверя", описанной в Апокалипсисе. Ведь вшивание под кожу микрочипа с номером или татуировка его на теле технологически эквивалентны формированию полной базы отпечатков пальцев всего населения.

Снять угрозу "печати зверя" удается только при переходе к новым высокоинтеллектуальным технологиям применения тайных, изменяемых самим человеком биометрических образов. К ним относятся динамические биометрические образы человека, которые имеют неограниченно высокую информативность и могут быть легко изменены по воле человека. Динамические биометрические образы могут быть получены механизмами анализа особенностей голоса, рукописного почерка, клавиатурного почерка [2, 3] и т.п.

Чтобы обеспечить дистанционную аутентификацию личности, необходимо привлекать биометрические технологии, способные безопасно взаимодействовать с другими высоконадежными механизмами, сопоставимыми по стойкости с криптографическими. При этом система должна быть дружественной к пользователям, а механизмы защиты – невидимыми для них. Стойкость защиты может быть и ниже криптографической (в зависимости от задачи и сферы применения), но она должна быть повсеместной для легитимных пользователей.

Однако при массовом использовании высоконадежных механизмов возникают проблемы распределения и хранения личных ключей доступа миллионов пользователей. Эту задачу не удается решить традиционными методами. Ведь все системы, использующие криптографические механизмы, весьма уязвимы, поскольку используют ключ – длинный код, который обычный человек практически не в силах запомнить. Поэтому ключи записываются на какой-либо физический носитель – специальным образом учтенные бланки, дискеты, пластиковые карточки, другие запоминающие устройства и т.д.

До тех пор, пока криптографические протоколы использовались только в интересах государственных структур, были приемлемыми такие методы сохранения ключей в тайне, как организация специальной охраны, сейфы и др. Однако с расширением круга лиц, пользующихся криптографическими технологиями, подобные решения стали слишком дорогими и "тяжелыми". При этом проблема полной дистанционной аутентификации личности остается открытой, поскольку не исключается кража (компрометация) ключа, в результате чего пользователем может оказаться совсем не то лицо, которое должно иметь доступ к информационным ресурсам.

Практически все страны со значимым научно-техническим потенциалом пытаются решать задачи безопасного хранения криптографических ключей доступа. Россия и США, являясь лидерами технологий защиты информации, открыто публикуют результаты своих исследований. Для решения этого вопроса США идут по пути использования нечеткой математики [4]. По материалам открытых источников американские ученые предлагают специализированные обогатители (fuzzy extractors), превращающие бедную неоднозначную размытую биометрическую информацию в сильный личный ключ пользователя. Однако устройств или просто действующих макетов данных устройств пока нигде не представлено, что говорит о том, что работы продвигаются успешно и их просто засекретили. Или наоборот: теоретически вопрос решаем, а практическая реализации довольна сложна. Ответы на эти вопросы даст время.

Российские специалисты предложили использовать системы полностью автоматической высоконадежной биометрико-нейросетевой аутентификации личности, как локальной, так и дистанционной, в открытом информационном пространстве. Россия в решении данного вопроса пошла более надежным, апробированным и дешевым в реализации путем применения больших и сверхбольших нейронных сетей, которые заранее обучаются преобразовывать размытые биометрические данные пользователя в его личный высоконадежный ключ по стойкости сопоставимый с криптографическим ключом [3]. В настоящее время в соответствии с ГОСТ Р 52633-2006 разработан программный хранитель секретов на основе биометрико-нейросетевых технологий. Сферы его применения – электронные паспорта, электронная торговля, цифровая подпись, электронный документооборот, системы доступа к информационным и иным ресурсам.

Обучение нейросети осуществляется на 15–20 примерах биометрического образа пользователя. После окончания процесса обучения программа информирует пользователя о стойкости программного нейросетевого "контейнера" – хранителя стойкого ключа (длина ключа – 256 бит). Если пользователя удовлетворяет стойкость "контейнера", то биометрические образы, служившие основой обучения нейросети, с компьютера удаляются. Тем самым, в отличие от западных технологий относительно "слабой" биометрии, где биометрический шаблон пользователя находится в компьютерной базе и может быть похищен, в предлагаемом методе в компьютере присутствуют только весовые коэффициенты нейросети, обученной на биометрических образах. Извлечение биометрического образа конкретного пользователя и его дальнейшее использование невозможно. Другое отличие российской технологии – использование "слабой, сильно размытой" информации динамической биометрии: рукописное написание и голосовое произношение слова (фразы)-пароля. Программный продукт используется совместно с карманными персональными компьютерами, коммуникаторами и другими типами ПЭВМ (www.pniei.penza.ru/prod/neiro.htm). Другим немаловажным показателем является низкая стоимость российского программного продукта.

ЛИТЕРАТУРА

1. **Болл Руд** и др. Руководство по биометрии. – М.: Техносфера, 2007.
2. **Волчихин В.И., Иванов А.И., Фунтиков В.А.** Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. – Пенза: Издательство Пензенского государственного университета, 2005.
3. ГОСТ Р 52633-2006 "Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации"
4. **Yevgeni Dodis, Rafail Ostrovsky, Leonid Reyzin, Adam Smith.** Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. – www.cs.bu.edu/~reyzin/fuzzy.html.
5. **Иванов А.И.** ГОСТ Р 52633-2006: Россией снята угроза "печати зверя" /В сборнике статей II Всероссийской научно-практической конференции "Антитеррористическая безопасность". – Пенза: Издательство Пензенского государственного университета, 2007, с.136–138.