УДК 519.711.3:343.98

Н.И. МАЗНИЧЕНКО, НЮАУ (г. Харьков)

ОБЛАСТИ ПРИМЕНЕНИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ БИОМЕТРИЧЕСКИХ СИСТЕМ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

Стаття присвячена практичним аспектам впровадження біометричних технологій, основним областям вживання біометрії, особливостям її використовування і підходам до побудови біометричних систем. Сформульовані критерії якості біометричних систем, методи їх оцінки і визначені вимоги для того або іншого вживання.

This article is devoted to the practical aspects of introduction of biometric technologies, basic regions of the use of biometric, features of its use and approaches to construction of the biometric systems. Formulated criteria of quality of the biometric systems, methods of their estimation and the requirements for every concrete application are definite.

Введение. В конце XX века интерес к биометрии значительно возрос. Основное достоинство биометрии – она позволяет идентифицировать человека с помощью его самого же. Сегодня стала очевидной необходимость точной идентификации в местах массового скопления людей, при контроле пропусков и сверке документов. В первую очередь проблема коснулась безопасности транспортных, а также государственных и межгосударственных систем – паспортных, визовых, таможенных, миграционных служб. Обычных методов контроля стало явно недостаточно. Все надежды теперь связаны с использованием биометрических технологий, позволяющих проверять личности огромного количества людей, проходящих через точку контроля [1].

Анализ литературы. Большое количество научных исследований и публикаций по данной теме свидетельствует о повышенном интересе к данному направлению. В 2002 г. было создано Русское биометрическое общество (http://www.biometrica.ru), сотрудники которого: Спиридонов И.Н., Дунаев Д.Ю., Климакин С.П., Петруненков А.А. внесли значительный вклад в становление теоретических основ данного направления. Серьезные исследования данной проблемы проводили так же ученые Шаров В. [2], Лакин Г.Ф. [3], Чернявский Ю.А. [4], Федоров В.Ю. [5] и др. Компании НПО "Информация" и "A4Vision" предлагают актуальные решения в области биометрических и интеллектуальных систем безопасности. Однако необходимо, рассмотрев накопленный опыт научных исследований и практических применений, более четко сформулировать основные направления в применении современных биометрических систем, принципы их построения, обозначить перспективные направления использования.

Цель статьи. Несмотря на лавинный и стремительный спрос на биометрию, необходимо объективно и взвешенно ответить на главный вопрос: "Насколько готовы сами технологии справиться с возложенными на них

задачами?" Необходимо сформулировать критерии качества биометрической системы, методы их оценки и определить требования для того или иного применения. Этому и посвящена данная статья.

Изложение основного материала. Под биометрическими технологиями понимают автоматические или автоматизированные методы распознавания личности человека по его биологическим характеристикам или проявлениям. Основные составляющие биометрического метода – это сканер для измерения биометрической характеристики и алгоритм, позволяющий сравнить ее с предварительно зарегистрированной той же характеристикой (так называемым биометрическим шаблоном). Возможны два режима работы системы – верификация (сравнение одного с одним) и идентификация (сравнение одного с многими). При всем теоретическом многообразии возможных биометрических методов (отпечаток пальца, геометрия кисти руки, форма лица, радужная оболочка глаза, сетчатка глаза) применимых на практике среди них немного. Основных методов три – распознавание по отпечатку пальца, по изображению лица (двухмерному или трехмерному – 2D- или 3D-фото) и по радужной оболочке глаза [6].

Рассмотрим области, в которых биометрия уже активно используется на протяжении нескольких лет, и отдельно остановимся на новых перспективных направлениях ее использования.

Компьютерная безопасность. В этой области биометрия используется для замены (или усиления) стандартной процедуры входа в различные программы по паролю, смарт-карте и т. д.

Самое распространенное решение на базе биометрических технологий – это идентификация (или верификация) по биометрическим характеристикам в корпоративной сети или при входе на рабочую станцию (персональный компьютер, ноутбук и т. д.) [7].

При защите рабочей станции создаются шаблоны биометрических данных (например, отпечатков пальцев) зарегистрированных пользователей, которые находятся в защищенном хранилище непосредственно на рабочей станции. После успешного прохождения процедуры идентификации пользователю предоставляется доступ.

При реализации технологии в корпоративной сети шаблоны биометрических данных всех пользователей сети хранятся централизованно на специально выделенном сервере аутентификации. При входе в сеть пользователь, проходя процедуру биометрической идентификации, работает непосредственно со специализированным сервером, на котором и проверяются предоставляемые идентификаторы. Выделение в структуре корпоративной сети отдельного сервера биометрической аутентификации позволяет хранить на таком сервере конфиденциальную информацию, доступ к которой будет предоставлен только по биометрическому идентифицирующему признаку владельца информации.

В данной области нашли применение следующие технологии

распознавания: отпечаток пальца, радужная оболочка глаза, голос, почерк, клавиатурный набор.

Торговля. В нашей стране эта область пока не развита, но на Западе получила достаточно широкое распространение. В первую очередь это касается распознавания отпечатка пальца и формы руки. Внедрение биометрии в торговле идет по следующим направлениям:

– в магазинах, ресторанах и кафе биометрические идентификаторы используются как средство идентификации покупателя и последующего снятия денег;

– в торговых автоматах и банкоматах как средство идентификации человека (взамен магнитных карточек или в дополнение к ним);

– в электронной коммерции биометрические идентификаторы используются как средство дистанционной идентификации через Интернет, а в сочетании со средствами криптографии дают электронным транзакциям очень высокий уровень защиты.

Системы контроля и управления доступом в помещения. Системы на базе биометрических технологий для контроля доступа (СКУД) в принципе аналогичны решениям для входа в сеть. Цифровые шаблоны биометрических характеристик человека заносятся в память дверного замка или турникета, после чего при каждом входе (выходе) человеку нужно пройти процедуру биометрической идентификации для открытия двери (отсканировать палец, сетчатку глаза или произнести кодовую фразу) [8].

В СКУД реализуются следующие технологии распознавания: отпечаток пальца, лицо, форма руки, радужная оболочка глаза, голос.

Иногда на основе таких систем дополнительно создается подсистема учета рабочего времени. В этих случаях используются биометрические замки с сетевой архитектурой или обычные системы биометрического сканирования.

Системы гражданской идентификации и автоматизированные дактилоскопические идентификационные системы (АДИС). Системами гражданской идентификации принято называть общегосударственные биометрические системы идентификации личности при выдаче документов, пересечении границ, распределении пособий и дотаций. В настоящее время такие системы получили самое широкое распространение, поскольку они стали использоваться при въезде в некоторые страны для проверки личности въезжающих [9]. В первую очередь это касается США, в ближайшее время похожую систему планирует ввести Европейский Союз и Россия. Страны-участницы Шенгенского соглашения уже договорились изменить формат въездных виз, в которые теперь будут записываться биометрические данные. Аналогичные программы начались во многих странах Азии.

Необходимо различать системы гражданской идентификации (по принятой в зарубежных странах терминологии, системы Civil ID) и криминалистические автоматизированные дактилоскопические идентификационные системы – АДИС (AFIS). Параметры этих систем

принципиально различаются.

В отличие от криминалистических приложений, которые требуют получения отпечатков всех десяти, гражданские приложения требуют изображений отпечатков двух пальцев. Одно из наиболее важных различий этих систем – полностью автоматический поиск и принятие решения в Civil ID-системах и необходимость работы высококвалифицированного эксперта криминалиста в криминалистических АДИС [10].

Комплексные системы. Это системы, сочетающие в себе системы первых трех классов. Например, совместное использование СКУД и компьютерной безопасности с единым для обеих систем сервером аутентификации, т. е. сотрудники компании регистрируются у администратора системы всего один раз, дальше ему автоматически назначаются все необходимые привилегии как на вход в помещение, так и на работу в корпоративной сети и ее ресурсы.

Кроме этих основных секторов применения, в настоящее время начинается активное использование биометрии и в других областях:

– игорный бизнес, казино. Биометрия используется по двум направлениям: проверка всех находящихся по "черным спискам" (аналог массовой идентификации по лицам, применяемой в аэропортах), а также как система идентификации и платежное средство постоянных клиентов;

– идентификация в мобильных устройствах, таких, как мобильные телефоны, КПК и т. д.;

– в транспорте как платежное средство;

– электронные системы голосования (используются вместо карточек);

– медицина. Биометрия применяется для идентификации медицинских работников при получении доступа к закрытым данным и для электронной подписи записей в истории болезни.

Общепринятых критериев, которые можно было использовать при построении биометрических систем в масштабах какого-либо предприятия, нет. Поэтому в этой статье будут даны только рекомендации, полученные из опыта внедрения биометрических систем.

Итак, первое, с чем необходимо определиться, – это непосредственно технология распознавания, которую предстоит использовать. Для этого нужно руководствоваться сочетанием двух критериев.

Точность технологии. Качественными показателями функционирования алгоритмов биометрической идентификации служат значения: FAR (False Acceptance Rate) – достоверность ошибочного распознавания, то есть достоверность того, что система спутает два индивидуума, признав "чужого" "своим"; FRR (False Rejection Rate) – достоверность ошибочного нераспознавания, то есть того, что система не распознает знакомого ей субъекта (достоверность не пропуска "своего").

На практике уменьшение FAR всегда приводит к уменьшению чувствительности метода или, что эквивалентное, к увеличению FRR [4]. Идеальные характеристики системы – это разнесенные показатели ошибки и

отказа идентификации, когда одновременно при большой надежности идентификации (ошибка 0,0001%) достигается отказ идентификации всего доли процента.

Показатель ошибки идентификации определяется выбранным подходом, качеством реализации и настройки алгоритмов идентификации. Для каждого конкретного производителя и его оборудования FAR и FRR указываются точно. Отметим, что показатели меняются в зависимости от производителя и погрешности тестирования, но важно то, что три метода распознавания – по отпечатку пальца, по трехмерному изображению лица, по радужной оболочке глаза – обладают сравнимой точностью. При этом распознавание по двухмерному изображению лица уступает перечисленным методам по точности на порядок, равно как и другие биометрические методы (распознавания по геометрии руки, по голосу и т. д.).

Удобство использования. Нужно предусмотреть, чтобы сотрудникам компании было удобно проходить биометрические процедуры идентификации в рамках решаемой задачи.

После выбора технологии предстоит выбрать изготовителя оборудования, которое удовлетворяло бы вашим требованиям, и, что не менее важно, представителя компании-производителя в стране.

Устойчивость к окружающей среде. Эксплуатационные качества разных биометрических методов сильно зависят от окружающих условий и могут терять стабильность при изменении этих условий. Так, сканеры отпечатков пальцев постоянно загрязняются и качество работы их падает, двухмерные методы распознавания лица сильно зависят от внешней освещенности и т. д.

Устойчивость к подделке. Биометрическая система должна быть устойчивой к подделке (несанкционированному доступу). Систему распознавания по двухмерному (2D) изображению лица можно легко "обмануть", предъявив фотографию из числа знакомых системе. Для получения несанкционированного доступа по отпечатку пальца бывает достаточно нанести графитовую пудру и надавить через тонкую пленку.

Стоимость системы. Вопреки мнению о дороговизне внедрения биометрических систем, за последние пять лет их цена в среднем снизилась в 2 – 3 раза. При оценке системы нужно учитывать, что ее стоимость складывается из многих составляющих. Например, для сетевой защиты – это считывающие устройства, сервер аутентификации и пользовательские лицензии к нему, услуги по внедрению и сопровождению и, если требуется, отдельно разработка модуля интеграции с каким-либо специальным корпоративным программным обеспечением.

Скорость работы биометрической системы. С этим критерием ситуация очевидна: чем быстрее пользователь распознается в системе, тем лучше. Нужно отметить, что скорость зависит от выбора метода распознавания: верификации или идентификации, так как очевидно, что сравнение шаблонов "один к одному" намного быстрее сравнения одного шаблона со всей базой

зарегистрированных.

Кроме этого, существует еще несколько критериев оценки биометрических систем, но они носят частный характер для каждой технологии.

Выводы. Применение биометрических технологий постепенно переходит из области альтернативы другим системам идентификации (карточным, парольным и т. д.) в области, в которых разворачивается конкуренция только между методами биометрической идентификации.

Одна из причин популярности биометрических систем сводится к объективной потребности заказчиков организовать современную, грамотно построенную систему безопасности у себя на предприятии, в офисе компании или в частном доме. Большинство прогнозов сводится к тому, что внедрение биометрических систем безопасности на отечественный рынок приобретет в скором будущем лавинный характер. Интенсивное развитие мультимедийных, цифровых технологий и, как следствие, их удешевление позволяют не только разработать принципиально новые подходы в проблеме идентификации личности, но и внедрить их в широкое повсеместное использование. В настоящий момент совершенствование биометрических технологий происходит ускоренными темпами. В первую очередь это приводит к тому, что повышается надёжность и снижается стоимость данных технологий.

Список литературы: 1. *Вакуленко А., Юхин А.* Биометрические методы идентификации личности: обыкновенный выбор // Сборник научных трудов 1 Международной научно-практической конференции "Мировой опыт применения биометрических решений в составе комплексных систем безопасности". – К.: "Информация-Украина". – 2006. – С. 79–82. **2.** *Шаров В.* Биометрические методы компьютерной безопасности // "BYTE". – 2005. – № 4. – С. 32–35. **3.** *Лакин Г.Ф.* Биометрия. Учебное пособие. – М.: Высшая школа. – 1990. – 223 с. **4.** *Чернявский Ю.А.* Способы анализа качественных характеристик автоматизированных дактилоскопических идентификационных систем. – М.: Политехник. – 2004. – 315 с. **5.** *Федоров В.Ю.* К вопросу об исследовании идентификационных признаков папиллярных узоров в АДИС // Проблемы совершенствования правоохранительной деятельности ОВД. Межвузовский сборник научных трудов. Ч.1. – М.: МЮИ МВД России. – 2000. – С. 36–39. **6.** *Животовский Л.А.* Популярная биометрия. – М.: Наука. – 1991. – 287 с. **7.** *Попов М.* Технологии биометрической идентификации // CHIP. – 2005. – № 9. – С. 45–47. **8.** *Умнов А.* Опыт применения биометрических решений в составе систем контроля доступа // Сборник научных трудов 1 Международной научно-практической конференции "Мировой опыт применения биометрических решений в составе комплексных систем безопасности". – К.: "Информация-Украина". – 2006. – С. 52–57. **9.** *Дудка В.* Опыт и перспективы применения биометрии в системах оперативной гражданской идентификации личности // Сборник научных трудов 1 Международной научно-практической конференции "Мировой опыт применения биометрических решений в составе комплексных систем безопасности". – К.: "Информация-Украина". – 2006. – С. 22–25. **10**. *Федоров В.Ю.* Об использовании оперативной идентификации в автоматизированных дактилоскопических учетах // История и современность экспертно-криминалистической службы. Межвузовский сборник научных трудов. – М.: МЮИИИ МВД России. – 1999. – С. 22–29.

Поступила в редакцию 30.03.2007